Re: What’s up Johnny?
Covert Content Attacks on Email End-To-End Encryption

Jens Müller, Marcus Brinkmann, Damian Poddebniak, Sebastian Schinzel, Jörg Schwenk
Remember EFAIL?
Remember EFAIL?

- Last year: EFAIL
Remember EFAIL?

• Last year: EFAIL
  – Major attack with a logo
Remember EFAIL?

• Last year: EFAIL
  – Major attack with a logo
  – Novel attack techniques targeting S/MIME + PGP
• Last year: EFAIL
  – Major attack with a logo
  – Novel attack techniques targeting S/MIME + PGP
• Today: non-crypto attacks
Remember EFAIL?

• Last year: EFAIL
  – Major attack with a logo
  – Novel attack techniques targeting S/MIME + PGP

• Today: non-crypto attacks
  – Targeting encryption and digital signatures
Overview

1. Introduction
2. Attacks on Encryption
3. Attacks on Signatures
4. Evaluation
5. Mitigation
1. Introduction
2. Attacks on Encryption
3. Attacks on Signatures
4. Evaluation
5. Mitigation
Technology's promise
I. “Strong crypto is virtually unbreakable.”
I. “Strong crypto is virtually unbreakable.”

II. “Digital signature will prevail. Math wins.”
I. “Strong crypto is virtually unbreakable.”
II. “Digital signature will prevail. Math wins.”

What if...

...claims I. and II. could be bypassed with a single reply to a benign looking email?
From: alice@good.com
To: johnny@good.com
Subject: Important news

Some ASCII text message...
From: alice@good.com
To: johnny@good.com
Subject: Important news

Some ASCII text message...
From: alice@good.com
To: johnny@good.com
Subject: Important news

Some ASCII text message…
From: alice@good.com
To: johnny@good.com
Subject: Important news

-----BEGIN PGP MESSAGE-----
...
-----END PGP MESSAGE-----
From: alice@good.com
To: johnny@good.com
Subject: Important news

-----BEGIN PGP MESSAGE-----
...
-----END PGP MESSAGE-----
From: alice@good.com
To: johnny@good.com
Subject: Important news

-----BEGIN PGP MESSAGE-----
...
-----END PGP MESSAGE-----
Multipart MIME email
From: alice@good.com
To: johnny@good.com
Content-type: multipart/mixed; boundary="XXX"

--XXX
Content-type: text/plain

Some ASCII text message...
--XXX
Content-type: text/plain

This is the 2nd part
--XXX--
From: alice@good.com
To: johnny@good.com

Content-type: multipart/mixed; boundary="XXX"

--XXX
Content-type: text/plain

Some ASCII text message...
--XXX
Content-type: text/plain

This is the 2nd part
--XXX--
Multipart MIME email

From: alice@good.com
To: johnny@good.com

Content-type: multipart/mixed; boundary="XXX"

--XXX
Content-type: text/plain

Some ASCII text message...

--XXX
Content-type: text/plain

This is the 2nd part

--XXX--
From: alice@good.com
To: johnny@good.com

Content-type: multipart/mixed; boundary="XXX"

--XXX

Content-type: text/plain

Some ASCII text message...

--XXX

Content-type: text/plain

This is the 2nd part

--XXX--
From: alice@good.com
To: johnny@good.com
Content-type: multipart/mixed; boundary="XXX"

--XXX
Content-type: text/plain
Some ASCII text message...
--XXX
Content-type: text/plain
This is the 2nd part
--XXX--
From: alice@good.com
To: johnny@good.com
Content-type: multipart/mixed; boundary="XXX"

--XXX
Content-type: text/plain
Some ASCII text message...
--XXX
Content-type: text/plain
This is the 2nd part
--XXX--
From: alice@good.com
To: johnny@good.com

Content-type: multipart/mixed; boundary="XXX"

--XXX

Content-type: text/html

<b>HTML</b> message...

--XXX

Content-type: application/pdf

%PDF-1.4 [...]

--XXX--
From: alice@good.com
To: johnny@good.com
Subject: Important news
Content-Type: application/pkcs7-mime

MIAGCSqGSIb3DQEHA6CAMIACAQAxggHJMIIB...
From: alice@good.com
To: johnny@good.com
Subject: Important news

Content-Type: application/pkcs7-mime

MIAGCSqGSIb3DQEHA6CAMIACAQAxggHJMIIB...
From: alice@good.com
To: johnny@good.com
Subject: Important news

Content-Type: application/pkcs7-mime

MIAGCSqGSIb3DQEHA6CAMIACAQAxggHJMIIB...
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
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

Today, we don’t care about the encryption scheme
Overview

1. Introduction
2. Attacks on Encryption
3. Attacks on Signatures
4. Evaluation
5. Mitigation
Overview

1. Introduction
2. Attacks on Encryption
3. Attacks on Signatures
4. Evaluation
5. Mitigation
Attacker model
• Eve has captured ciphertext
Attacker model

• Eve has captured ciphertext
• Can modify email structure
Attacker model

- Eve has captured ciphertext
- Can modify email structure
- Can re-send it to the victim
• Eve has captured ciphertext
• Can modify email structure
• Can re-send it to the victim
  – Either to recipient or sender
Attacker model

- Eve has captured ciphertext
- Can modify email structure
- Can re-send it to the victim
  - Either to recipient or sender
  - Both can decrypt the email
Covert content attack: Decryption oracle

Attacker

Decryption oracle $\omega$
Covert content attack: Decryption oracle

"What's up Johnny?"

Attacker

visible

Decryption oracle $\omega$
Covert content attack: Decryption oracle

"What's up Johnny?" || $\text{enc}_\omega(m)$

Attacker

visible

covert

Decryption oracle $\omega$
Covert content attack: Decryption oracle

Attacker

"What's up Johnny?" || $\text{enc}_\omega(m)$

"I'm fine, thanks." || $m$

Decryption oracle $\omega$

visible

covert
From: alice@good.com
To: johnny@good.com
Content-Type: application/pkcs7-mime

MIAGCSqGSIb3DQEHA6CAMIACAQAxggHJMIIB...
To: johnny@good.com

Content-Type: application/pkcs7-mime

MIAGCSqGSIb3DQEHA6CAMIACAQAxggHJMIIB...
From: eve@evil.com
To: johnny@good.com
Content-Type: application/pkcs7-mime

MIAGCSqGSIb3DQEHA6CAMIACAQAxggHJMIIB...
From: eve@evil.com
To: johnny@good.com

Content-Type: application/pkcs7-mime

MIAGCSqGSIb3DQEHA6CAMIACAQAxggHJMIIB...
From: eve@evil.com
To: johnny@good.com

Content-Type: application/pkcs7-mime

MIAGCSqGSIb3DQEHA6CAMIACAQAxggHJMIIB...
Decryption oracle

From: eve@evil.com
To: johnny@good.com

Content-type: multipart/mixed; boundary="XXX"

--XXX

--XXX

Content-Type: application/pkcs7-mime

MIAGCSqGSIb3DQEHA6CAMIACAQAxggHJMIIB...

--XXX--
Decryption oracle

From: eve@evil.com
To: johnny@good.com

Content-type: multipart/mixed; boundary="XXX"

--XXX

Content-type: text/plain

What's up Johnny?

--XXX

Content-Type: application/pkcs7-mime

MIAGCSqGSIb3DQEHA6CAMIACAQAxggHJMIIB...

--XXX--
From: eve@evil.com
To: johnny@good.com

Content-type: multipart/mixed; boundary="XXX"

--XXX
Content-type: text/plain

What's up Johnny?

--XXX
Content-Type: application/pkcs7-mime

MIAGCSqGSIb3DQEHA6CAMIACAQAxggHJMIIB...

--XXX--
Decryption oracle

From: eve@evil.com
To: johnny@good.com

Content-type: multipart/mixed; boundary="XXX"

--xxx

Content-type: text/plain

What's up Johnny?

--xxx

Content-type: text/plain

Secret message, for Johnny's eyes only...

--xxx--
From: eve@evil.com
To: johnny@good.com

Content-type: multipart/mixed; boundary="XXX"

--XXX

Content-type: text/plain

What's up Johnny?

--XXX

Content-type: text/plain

Secret message, for Johnny's eyes only...

--XXX--
Decryption oracle

From: eve@evil.com
To: johnny@good.com
Content-type: multipart/mixed; boundary="XXX"

--XXX
Content-type: text/plain
What's up Johnny?
--XXX
Content-type: text/plain
Secret message, for Johnny's eyes only...
--XXX--
From: eve@evil.com
To: johnny@good.com

Content-type: multipart/mixed; boundary="XXX"

--XXX

Content-type: text/plain

What's up Johnny?

--XXX

Content-type: text/plain

Secret message, for Johnny's eyes only...

--XXX--
Decryption oracle

From: eve@evil.com
To: johnny@good.com

Content-type: multipart/mixed; boundary="XXX"

--XXX

Content-type: text/plain

What's up Johnny?

--XXX

Content-type: text/plain

Secret message, for Johnny's eyes only...

--XXX--
From: eve@evil.com
To: johnny@good.com

Content-type: multipart/mixed; boundary="XXX"

--XXX

Content-type: text/html

What's up Johnny? <!--

--XXX

Content-type: text/plain

Secret message, for Johnny's eyes only...

--XXX--
From: eve@evil.com
To: johnny@good.com

Content-type: multipart/mixed; boundary="XXX"

--XXX

Content-type: text/html

What's up Johnny? <!--

--XXX

Content-type: text/plain

Secret message, for Johnny's eyes only...

--XXX--

Decryption oracle
Decryption oracle

From: eve@evil.com
To: johnny@good.com

Content-type: multipart/mixed; boundary="XXX"

--XXX

Content-type: text/html

What's up Johnny? <img src="cid:part2">

--XXX

Content-ID: <part2>

Secret message, for Johnny's eyes only...

--XXX--
From: eve@evil.com
To: johnny@good.com

Content-type: multipart/mixed; boundary="XXX"

--XXX

Content-type: text/plain

What's up Johnny?

--XXX

Content-Disposition: attachment

Secret message, for Johnny's eyes only...

--XXX--
Overview

1. Introduction
2. Attacks on Encryption
3. Attacks on Signatures
4. Evaluation
5. Mitigation
Overview

1. Introduction
2. Attacks on Encryption
3. Attacks on Signatures
4. Evaluation
5. Mitigation
Covert content attack: Signing oracle
Covert content attack: Signing oracle

"What's up Johnny?"

Attacker

visible

Signing oracle $\omega$
Covert content attack: Signing oracle

"What's up Johnny?" || "I hereby declare war."

Attacker

visible

covert

Signing oracle ω
Covert content attack: Signing oracle

"What's up Johnny?" || "I hereby declare war."

\[ \text{sig}_\omega( "I'm fine, thanks." || "I hereby declare war." ) \]

Attacker

visible

covert

Signing oracle \( \omega \)
Covert content attack: Signing oracle

"What's up Johnny?" || "I hereby declare war."

$\text{sig}_\omega(\text{"I'm fine, thanks."} || \text{"I hereby declare war."})$

$\text{sig}_\omega(\text{"I'm fine, thanks."} || \text{"I hereby declare war."})$

Signing oracle $\omega$

Third party
What's up Johnny?
I hereby declare war.
From: eve@evil.com
To: johnny@good.com
Content-type: text/html

What's up Johnny?

<div class="covert">I hereby declare war. </div>
From: eve@evil.com
To: johnny@good.com
Content-type: text/html

What's up Johnny?

<div class="covert">I hereby declare war.</div>
From: eve@evil.com
To: johnny@good.com
Content-type: text/html

What's up Johnny?

I hereby declare war.
From: eve@evil.com
To: johnny@good.com
Content-type: text/html

What's up Johnny?
<div class="covert">I hereby declare war.</div>
I'm fine, thanks.

On 01/05/19 09:53, Eve wrote:
> What's up Johnny?
I'm fine, thanks.

On 01/05/19 09:53, Eve wrote:
> What's up Johnny?
Re: What's up Johnny?

I'm fine, thanks.

On 01/05/19 09:53, Eve wrote:
> What's up Johnny?

Reply email sent from Johnny’s mobile phone
I'm fine, thanks.

On 01/05/19 09:53, Eve wrote:
> What's up Johnny?

I hereby declare war.

---

Reply email sent from Johnny’s mobile phone

Signed email received on a desktop device
Conditional rules
Conditional rules

• Targeting device type (@media)
Conditional rules

- Targeting device type (@media)
- Targeting email client (@supports)
Conditional rules

• Targeting device type (@media)
• Targeting email client (@supports)
• Targeting user account (@document)
Conditional rules

• Targeting device type (@media)
• Targeting email client (@supports)
• Targeting user account (@document)
Overview

1. Introduction
2. Attacks on Encryption
3. Attacks on Signatures
4. Evaluation
5. Mitigation
<table>
<thead>
<tr>
<th>OS</th>
<th>Client</th>
<th>Decryption</th>
<th>Signatures</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>S/MIME</td>
<td>PGP</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows</td>
<td>Thunderbird</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Outlook</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Win. 10 Mail</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Win Live Mail</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The Bat!</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Postbox</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>eM Client</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Linux</td>
<td>KMmail</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Evolution</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Trojitá</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Claws</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Mutt</td>
<td></td>
<td></td>
</tr>
<tr>
<td>macOS</td>
<td>Apple Mail</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>MailMate</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Airmail</td>
<td></td>
<td></td>
</tr>
<tr>
<td>iOS</td>
<td>Mail App</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Android</td>
<td>K-9 Mail</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>R2Mail2</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>MailDroid</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Nine</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web</td>
<td>Exchange/OWA</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Roundcube</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Horde/IMP</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Mailpile</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Decryption oracles
- ● Plaintext can be completely hidden
- ○ Plaintext merged with attacker-text

Signature oracles
- ● Covert rules kept in reply message
- ○ Covert rules only for received mail
- ○ No vulnerabilities found
  - Cryptosystem not available
<table>
<thead>
<tr>
<th>OS</th>
<th>Client</th>
<th>Decryption</th>
<th>Signatures</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>S/MIME</td>
<td>PGP</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows</td>
<td>Thunderbird</td>
<td>●</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Outlook</td>
<td>○</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Win. 10 Mail</td>
<td>○</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Win Live Mail</td>
<td>○</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The Bat!</td>
<td>○</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Postbox</td>
<td>●</td>
<td></td>
</tr>
<tr>
<td></td>
<td>eM Client</td>
<td>○</td>
<td></td>
</tr>
<tr>
<td>Linux</td>
<td>KMail</td>
<td>○</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Evolution</td>
<td>○</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Trojitá</td>
<td>○</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Claws</td>
<td>●</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Mutt</td>
<td>○</td>
<td></td>
</tr>
<tr>
<td>macOS</td>
<td>Apple Mail</td>
<td>●</td>
<td></td>
</tr>
<tr>
<td></td>
<td>MailMate</td>
<td>●</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Airmail</td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>iOS</td>
<td>Mail App</td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>Android</td>
<td>K-9 Mail</td>
<td>–</td>
<td></td>
</tr>
<tr>
<td></td>
<td>R2Mail2</td>
<td>○</td>
<td></td>
</tr>
<tr>
<td></td>
<td>MailDroid</td>
<td>○</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Nine</td>
<td>○</td>
<td></td>
</tr>
<tr>
<td>Web</td>
<td>Exchange/OWA</td>
<td>○</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Roundcube</td>
<td>–</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Horde/IMP</td>
<td>○</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Mailpile</td>
<td>–</td>
<td></td>
</tr>
</tbody>
</table>

**Decryption oracles**

- ● Plaintext can be completely hidden
- ○ Plaintext merged with attacker-text

**Signature oracles**

- ● Covert rules kept in reply message
- ○ Covert rules only for received mail

- ○ No vulnerabilities found
  - Cryptosystem not available
<table>
<thead>
<tr>
<th>OS</th>
<th>Client</th>
<th>Decryption</th>
<th>Signatures</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>S/MIME</td>
<td>PGP</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows</td>
<td>Thunderbird</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>Outlook</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td></td>
<td>Win. 10 Mail</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td></td>
<td>Win Live Mail</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td></td>
<td>The Bat!</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td></td>
<td>Postbox</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>eM Client</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Linux</td>
<td>KMail</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>Evolution</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td></td>
<td>Trojita</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td></td>
<td>Claws</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td></td>
<td>Mutt</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>macOS</td>
<td>Apple Mail</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>MailMate</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>Airmail</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>iOS</td>
<td>Mail App</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>K-9 Mail</td>
<td>–</td>
<td>○</td>
</tr>
<tr>
<td></td>
<td>R2Mail2</td>
<td>○</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>MailDroid</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td></td>
<td>Nine</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Web</td>
<td>Exchange/OWA</td>
<td>○</td>
<td>–</td>
</tr>
<tr>
<td></td>
<td>Roundcube</td>
<td>–</td>
<td>○</td>
</tr>
<tr>
<td></td>
<td>Horde/IMP</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td></td>
<td>Mailpile</td>
<td>–</td>
<td>○</td>
</tr>
</tbody>
</table>

**Decryption oracles**
- ● Plaintext can be completely hidden
- ○ Plaintext merged with attacker-text

**Signature oracles**
- ● Covert rules kept in reply message
- ○ Covert rules only for received mail
- ○ No vulnerabilities found
- – Cryptosystem not available
<table>
<thead>
<tr>
<th>OS</th>
<th>Client</th>
<th>Decryption</th>
<th>Signatures</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>S/MIME</td>
<td>PGP</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td></td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Windows</td>
<td>Thunderbird</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>Outlook</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td></td>
<td>Win. 10 Mail</td>
<td>○</td>
<td>–</td>
</tr>
<tr>
<td></td>
<td>Win Live Mail</td>
<td>○</td>
<td>–</td>
</tr>
<tr>
<td></td>
<td>The Bat!</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td></td>
<td>Postbox</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>eM Client</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>KMail</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Linux</td>
<td>Evolution</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td></td>
<td>Trojitéá</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td></td>
<td>Claws</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td></td>
<td>Mutt</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Apple Mail</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>macOS</td>
<td>MailMate</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>Airmail</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Mail App</td>
<td>●</td>
<td>–</td>
</tr>
<tr>
<td>iOS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>K-9 Mail</td>
<td>–</td>
<td>○</td>
</tr>
<tr>
<td>Android</td>
<td>R2Mail2</td>
<td>○</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>MailDroid</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td></td>
<td>Nine</td>
<td>○</td>
<td>–</td>
</tr>
<tr>
<td></td>
<td>Exchange/OWA</td>
<td>○</td>
<td>–</td>
</tr>
<tr>
<td></td>
<td>Roundcube</td>
<td>–</td>
<td>○</td>
</tr>
<tr>
<td></td>
<td>Horde/IMP</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td></td>
<td>Mailpile</td>
<td>–</td>
<td>○</td>
</tr>
</tbody>
</table>

**Decryption oracles**
- ● Plaintext can be completely hidden
- ○ Plaintext merged with attacker-text

**Signature oracles**
- ● Covert rules kept in reply message
- ○ Covert rules only for received mail
- ○ No vulnerabilities found
- – Cryptosystem not available
<table>
<thead>
<tr>
<th>OS</th>
<th>Client</th>
<th>Decryption</th>
<th>Signatures</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>S/MIME</td>
<td>PGP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Windows</td>
<td>Linux</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Thunderbird</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>Outlook</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td></td>
<td>Win. 10 Mail</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td></td>
<td>Win Live Mail</td>
<td>○</td>
<td>–</td>
</tr>
<tr>
<td></td>
<td>The Bat!</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td></td>
<td>Postbox</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>eM Client</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td></td>
<td>KMail</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td></td>
<td>Evolution</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td></td>
<td>Trojita</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td></td>
<td>Claws</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td></td>
<td>Mutt</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td></td>
<td>Apple Mail</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>MailMate</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>Airmail</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>K-9 Mail</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td></td>
<td>R2Mail2</td>
<td>○</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>MailDroid</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td></td>
<td>Nine</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td></td>
<td>Exchange/OWA</td>
<td>○</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>Roundcube</td>
<td>–</td>
<td>○</td>
</tr>
<tr>
<td></td>
<td>Horde/IMP</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td></td>
<td>Mailpile</td>
<td>–</td>
<td>○</td>
</tr>
</tbody>
</table>

**Decryption oracles**
- ● Plaintext can be completely hidden
- ○ Plaintext merged with attacker-text

**Signature oracles**
- ● Covert rules kept in reply message
- ○ Covert rules only for received mail

- ○ No vulnerabilities found
  - Cryptosystem not available
<table>
<thead>
<tr>
<th>OS</th>
<th>Client</th>
<th>Decryption</th>
<th>Signatures</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>S/MIME</td>
<td>PGP</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows</td>
<td>Thunderbird</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>Outlook</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td></td>
<td>Win. 10 Mail</td>
<td>○</td>
<td>–</td>
</tr>
<tr>
<td></td>
<td>Win Live Mail</td>
<td>○</td>
<td>–</td>
</tr>
<tr>
<td></td>
<td>The Bat!</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td></td>
<td>Postbox</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>eM Client</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Linux</td>
<td>KMail</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td></td>
<td>Evolution</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td></td>
<td>Trojitá</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td></td>
<td>Claws</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td></td>
<td>Mutt</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>macOS</td>
<td>Apple Mail</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>MailMate</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>Airmail</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>IOS</td>
<td>Mail App</td>
<td>●</td>
<td>–</td>
</tr>
<tr>
<td>Android</td>
<td>K-9 Mail</td>
<td>–</td>
<td>○</td>
</tr>
<tr>
<td></td>
<td>R2Mail2</td>
<td>○</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>MailDroid</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td></td>
<td>Nine</td>
<td>○</td>
<td>–</td>
</tr>
<tr>
<td>Web</td>
<td>Exchange/OWA</td>
<td>○</td>
<td>–</td>
</tr>
<tr>
<td></td>
<td>Roundcube</td>
<td>–</td>
<td>○</td>
</tr>
<tr>
<td></td>
<td>Horde/IMP</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td></td>
<td>Mailpile</td>
<td>–</td>
<td>○</td>
</tr>
</tbody>
</table>

**Decryption oracles**

- ● Plaintext can be completely hidden
- ○ Plaintext merged with attacker-text

**Signature oracles**

- ● Covert rules kept in reply message
- ○ Covert rules only for received mail
- ○ No vulnerabilities found
  - Cryptosystem not available
1. Introduction
2. Attacks on Encryption
3. Attacks on Signatures
4. Evaluation
5. Mitigation
1. Introduction
2. Attacks on Encryption
3. Attacks on Signatures
4. Evaluation
5. Mitigation
Decryption oracles
Decryption oracles

- Accepting ASCII text only
Decryption oracles

• Accepting ASCII text only
Decryption oracles

- Accepting ASCII text only
- Enforcing digital signatures
Decryption oracles

- Accepting ASCII text only
- Enforcing digital signatures
Decryption oracles

- Accepting ASCII text only
- Enforcing digital signatures
- Warn on partial encryption
Decryption oracles

- Accepting ASCII text only
- Enforcing digital signatures
- Warn on partial encryption
Decryption oracles

- Accepting ASCII text only
- Enforcing digital signatures
- Warn on partial encryption
- All-or-Nothing Encryption
Decryption oracles

- Accepting ASCII text only
- Enforcing digital signatures
- Warn on partial encryption
- All-or-Nothing Encryption

Root causes: long-term keys + ciphertext usage out-of-context
Signing oracles
Signing oracles

- Dropping CSS Support
Signing oracles

• **Dropping CSS Support**
Signing oracles

- Dropping CSS Support
- Only ASCII Text in replies
Signing oracles

- Dropping CSS Support
- Only ASCII Text in replies
- Remove styles from replies
Conclusion

• Crypto is not enough, bypasses exist
Conclusion

- Crypto is not enough, bypasses exist
- 22 of 24 tested clients are vulnerable
Conclusion

- Crypto is not enough, bypasses exist
- 22 of 24 tested clients are vulnerable
- Building security on top of email is hard
Conclusion

• Crypto is not enough, bypasses exist
• 22 of 24 tested clients are vulnerable
• Building security on top of email is hard

Thank you! Questions?
Exploits: github.com/RUB-NDS/Covert-Content-Attacks
## HTML and CSS support in various email clients

<table>
<thead>
<tr>
<th>HTML</th>
<th>CSS styles</th>
<th>blinding options</th>
<th>conditional rules</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>view reply external internal inline display visibility opacity clip-path position color font-size</td>
<td>media @supports @document other</td>
<td></td>
</tr>
<tr>
<td><strong>Windows</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thunderbird</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Outlook 2016</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Win. 10 Mail</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>W. Live Mail</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The Bat!</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Postbox</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>eM Client</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Linux</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>KMail</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Evolution</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trojita</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Claws</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mutt</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Mac</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Apple Mail</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MailMate</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Airmail</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>iOS</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mail App</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Android</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>K-9 Mail</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>R2Mail2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MailDroid</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nine</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exchange/OWA</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Roundcube</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Horde/IMP</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mailpile</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

○ Not supported by client ● Supported in default settings ○ Supported in non-default settings
Proprietary conditional features

```html
<html><head>
<!--[if IE]><style>.wlm {color: red;}</style><![endif]--> <!-- Windows Live Mail -->
<!--[if mso]><style>.ol {color: red;}</style><![endif]--> <!-- Outlook / W10Mail -->
<style>
.ExternalClass .owa, [owa] .owa {color: red;}
/* Exchange (OWA) */
moz-text-html .tb {color: red;}
/* Thunderbird */
</style>
</head>
<body>
<div class="wlm">RED text only in Windows Live Mail</div>
<div class="ol">RED text only in Outlook / W10Mail</div>
<div class="owa">RED text only in Exchange (OWA)</div>
<div class="tb">RED text only in Thunderbird</div>
</body></html>
```
## Blinding options

<table>
<thead>
<tr>
<th>property</th>
<th>show</th>
<th>hide</th>
</tr>
</thead>
<tbody>
<tr>
<td>display</td>
<td>initial;</td>
<td>none;</td>
</tr>
<tr>
<td>visibility</td>
<td>visible;</td>
<td>hidden;</td>
</tr>
<tr>
<td>opacity</td>
<td>1;</td>
<td>0;</td>
</tr>
<tr>
<td>clip-path</td>
<td>initial;</td>
<td>polygon(0px 0px, 0px 0px, 0px 0px, 0px 0px, 0px 0px);</td>
</tr>
<tr>
<td>position</td>
<td>static;</td>
<td>absolute; top: -9999px; left: -9999px;</td>
</tr>
<tr>
<td>color</td>
<td>initial;</td>
<td>transparent;</td>
</tr>
<tr>
<td>font-size</td>
<td>initial;</td>
<td>0;</td>
</tr>
</tbody>
</table>

Table 1: CSS properties to hide text.