Session-6: MIME & PGP

What is PGP/Inline?

One approach to encrypt an email with PGP is to encrypt everything separately. This means that the message body and attachments are individually encrypted and signed. The benefit of this approach is that your recipient can use email clients that don’t support PGP encryption and use third party tools to decrypt the message, by copying the message body and/or downloading the attachments and using a tool like gpg to decrypt each one. However, because the message body and attachments are encrypted separately, this approach leaks information about the type and name of each attachment.

For historical reasons PGP/Inline doesn’t support sending HTML messages, so all PGP/Inline messages will be send in plain text.

Here is a sample PGP/Inline message:

```
Feedback-ID:
4pmPTj6JCqHsPH6LT3lnEhaUCPW3Kp_HNgUt_gfHN7Ck5LIN2KOTVUuznpq6wtEKqZ_gT7bMk_aJFB-nNQIg6Q==:Ex
t:ProtonMail
MIME-Version: 1.0
Content-Type: multipart/mixed;
        boundary="b1_046445deb82ecf7cef825fc3d254d9ed"

This is a multi-part message in MIME format.

--b1_046445deb82ecf7cef825fc3d254d9ed
Content-Type: text/plain; charset=UTF-8

-----BEGIN PGP MESSAGE-----
Version: ProtonMail
Comment: https://protonmail.com

wcFMA6wMBnJ9eG2kAQ/+L9wlGmvUhex26eAVOSdEDjUil/7jqnBALMULYA/T
6d5+NBuYMEN5PEBBBu2yu...NNHNHNlevr5aCwe!4qKLEopj75WVOZLjzleg
i3Jjb13JI1GOaGAjSs9wgPtlcjAg/ZNI2xayvllntKYWawfycw==
=cbuf
-----END PGP MESSAGE-----



--b1_046445deb82ecf7cef825fc3d254d9ed
Content-Type: application/octet-stream; name="attachment.txt.pgp"
Content-Disposition: attachment; filename="attachment.txt.pgp"

-----BEGIN PGP MESSAGE-----
Version: ProtonMail
Comment: https://protonmail.com

wcFMA6wMBnJ9eG2kAQ/9EuQ5oDjKOESIMY8xO6aCLWvxDMDLYhtOBr7LV7+KHrIT1KOhn5az4a3j
wtIp/T9iewzAJ8R/X9MMn+LPK2...pXN4u4Ntum7pdrH3XIldq8eKeKyUI17CGeS4x2kM7Qeha10
RbPUtwI2chE8uP6tvh/aqqke+E5mqA==
=dbaf
-----END PGP MESSAGE-----


--b1_046445deb82ecf7cef825fc3d254d9ed
Content-Type: application/pgp-signature; name="attachment.txt.sig"
Content-Disposition: attachment; filename="attachment.txt.sig"

-----BEGIN PGP SIGNATURE-----
wsBcBAABCAAQBQJaqBsFCRAbAnUMVNTNFqAApDYH/jSEJlIDMlHOpiFpWahjMEsnlxMIsBcncCh+
7KBk+zgocj7dmyzBXfQU7Yn/S2...9hnQQuLqFq6y7/sAU/wMmf/Ifji4BeV8nSKYnKEza7OFWtp
8nQ=
=5jab

-----END PGP SIGNATURE-----

--b1_046445deb82ecf7cef825fc3d254d9ed--
```

What is PGP/MIME?

A newer approach is PGP/MIME, which in contrast to PGP/Inline, PGP/MIME encrypts and signs the message, including attachments, as a whole.

An advantage to this scheme is that the message structure, like attachment metadata, is not leaked to someone who intercepts the encrypted message. PGP/MIME also tends to be less intrusive when displaying message signatures in clients that do not support PGP. However, to be able to read just the message body, it is necessary to download the whole message, including all attachments, because everything is encrypted together.

Unlike PGP/Inline, most clients support PGP/MIME in combination with HTML messages.

Encrypting with PGP/MIME will often generate a message like this:

```
MIME-Version: 1.0
Content-Type: multipart/encrypted; protocol="application/pgp-encrypted";
boundary="----------------------ff28bdd854f2b3f63b9e9c0afa07f1ae"; charset=UTF-8

------------------------ff28bdd854f2b3f63b9e9c0afa07f1ae
Content-Type: application/pgp-encrypted
Content-Description: PGP/MIME version identification

Version: 1

------------------------ff28bdd854f2b3f63b9e9c0afa07f1ae
Content-Type: application/octet-stream; name="encrypted.asc"
Content-Description: OpenPGP encrypted message
Content-Disposition: inline; filename="encrypted.asc"

-----BEGIN PGP MESSAGE-----
Version: ProtonMail
Comment: https://protonmail.com

wV4D+Z2CfIhvAcoSAQdAPGJCfV6Y9SaUDBJ2EBdr16f80wwkLGttEuTy2yPE
UBgwpLwlY8tkXClg3dcD5S3uci9zt3HN...N7LH0Gkq+gE5wYz8ThRTtX2Eu
Q5fp2JywHJAQYDvYL6iJsgwXRR3PM45DlBAtuTHowQ==
=Jtuy
-----END PGP MESSAGE-----


------------------------ff28bdd854f2b3f63b9e9c0afa07f1ae--
```

As shown above, this generates one big attachment called **encrypted.asc**, so anybody who sees this has no information about what may be inside this message.

After decrypting **encrypted.asc**, the following data can be found:

```
Content-Type: multipart/mixed;
        boundary="b1_7333dfe2b36a8ed0da4083ae371e83dd"

This is a multi-part message in MIME format.

--b1_7333dfe2b36a8ed0da4083ae371e83dd
Content-Type: text/html; charset=UTF-8
Content-Transfer-Encoding: base64

LS0tLS1CRUdJTiBQR1AgTUVTU0FHRS0tLS0tDQpWZXJzaW9uOiBQcm90b25NYWlsDQpDb21tZW50
OiBodHRwczovL3Byb3...AfKVklHKlFlQS96SUkNCjFkdkMNCjlJN1dkDQotLS0tLUVORCBQR1Ag
TUVTU0FHRS0tLS0tDQo=


--b1_7333dfe2b36a8ed0da4083ae371e83dd
Content-Type: application/octet-stream; name="attachment.png"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="attachment.png"

wV4D+Z2CfIhvAcoSAQdAYJXia5BajO6xr3eyJ4B/dDIgl0QoiixYFtXV5NX2vkYwFgwfbsrUcdP/
xkQyz7LCO5ZQt/6l5s7Sx...KVX2aG37JAHaze22YGs3H+VCl0lKqmYK3pdki+hyd82oNQaSG5bu
ZCYbp2SiTvhK3Tv9iqhrKvuaZiSE

--b1_7333dfe2b36a8ed0da4083ae371e83dd--
```