



PGP Forum

forums.pgpsupport.com

[FAQ](#) [Search](#) [Memberlist](#) [Usergroups](#)

[Profile](#) [You have no new messages](#) [Log out \[robert baskerville \]](#)

Be Afraid! First Transplanted PGP Signature Enclosed....



[Reply to topic](#)

[PGP Forum Forum Index -> Certified PGP Engineers](#)

[View previous topic](#) :: [View next topic](#)**Author****robert baskerville**

Joined: 23 Dec 2003
 Posts: 900
 Location: Universidad
 Autònoma Barcelona

Message

Posted: Fri Aug 20, 2004 1:37 am Post subject: Be Afraid! First Transplanted PGP Signature Enclosed....

 [quote](#)  [edit](#)  

Thought I'd better make my 900th post something special so....

Enclosed you will find what is, I believe, the first published example of transplanting a PGP Signature from ONE entity to ANOTHER without breaking it....

Background to this is [here](#) discussing the collisions in MD5.

This little experiment just brought it home with a bit of a thump though.

Take these two data files:

```

begin 644 file1.dat
MfS= 1P1L119MfM= 1P= *H0+2IG2D0' 18WCE7E8K308725' H0B0.E
M:4R=7%2E27'8B 7:W0B#45818+ <-c076c1-877A8E=4U+16'0,01#* 1
P50:7'8A*2=-_345718Z'W2+4957.0TR0Q=+8L8C6#473'.
end
begin 644 file2.dat
MfS= 1P1L119MfM= 1P= *H0+2IG2D0' 18WCE7E8K308725' H0B0.E
M:4R=7%2E27'8B 7:W0B#45818+ <-c076c1-877A8E=4U+16'0,01#* 1
P50:7'8A*2=-_345718Z'W2+4957.0TR0Q=+8L8C6#473'.
end

```

uudecode these two to get file1.dat and file2.dat

Now here is a PGP signature made with my old Legacy RSA PGP Key (available from the public keyservers):

-----BEGIN PGP SIGNATURE-----

Version: PGP 8.1

Comment: www.vistorm.com/pgp

iQCVAwUAQSU1bszvJGZSHZ+5AQHDLAQAsMQAzid5xezdDtb4oEWq/W4AcUNQIU4d
 spl6amEn0EK+iNXVLCbq6FIF7NYmYK0upwMx58V7KjJXwd7Kg/dNLv+yLoQCSHNI
 zXi3O63C38W4RxJRsw8teyS+Qm9rKapNfDIfwKqrBUBWSviTZ/H2zyfdIXdhIAZS
 LWkO+HOT28E=
 =y0Di
 -----END PGP SIGNATURE-----

Here is the question:

Q: WHICH FILE DID I SIGN?

A: you cannot tell because the signature verifies for BOTH files despite the two files being different....

Note that this Legacy RSA key is 1024 bit but that the SIZE of the key is irrelevant - the same would work for a 512 bit or a 2048 bit key since the problem lies with the MD5 hashing.

(You can see the files file1.dat and file2.dat are different if you "diff" them or compare SHA-1 hashes, or just read the bytes)

Q: WHAT does this mean?

A: using Legacy RSA Keys for signatures is a Bad Thing(tm) in some circumstances

(only) now

Here is a signature I made on the same file as the first signature, but using an RSA/RSA key:

-----BEGIN PGP SIGNATURE-----

Version: PGP 8.1

Comment: www.vistorm.com/pgp

```
iQGVAwUAQSU2paLvtZXFYwUMAQKtFwwAh/GZGocd/eFqq/Q1CZSgfc01VvbawrhK
yAvCuy1GfvdSFrafIp+L1MHQxey+AcxCGUIzIqh2Oa7W/EWP80ef3ubhn9fXEXfR
1MUFsGOql7acTOcvGNdfau57XsXL1+dUcXvZhMtZ4lckQIFZe4SEdQtoaPIKU6Gy
+QEDDyq5+He9XX5jZnsho2pMMufNOiseZivNZFZIHje9QS2IC/5gPou6il+JwWJY
XvWGt9rxPCmlEbHyy0iOb4BpbRapZIA9d6VQPtOGMiraoC3Lo/IQC1dZsK2yhQt+
mLsMRAjoS7Rt/eUv6Q4UhVo/TA624W7JvytgMq5Hw/2Rky80e9UtFVI64ZKO3Mc5
jmlhslfTzifpTnaRn0w5KtJF2AJH5dprpu0zsJAeE3GeAN+hU8smze9x7xGThVK6
4pO1Pvx+U6cY2Rn09/L6M7XiBgzB1Pq1vbzeb/gkgIzvhofkxjDWMEnm5AZx9hHC
rf/1HkBoZHqVLPkqoHRmJfQXXmIQ/0lt
=4Wbv
-----END PGP SIGNATURE-----
```

NOW you can see which file I signed....

Q: what does this mean for S/MIME signatures?

Q: what does this mean for x.509 certs?

Whilst this is a logical outcome of the MD5 collision, it is something I never expected to see myself....

Robert Baskerville
Principal Security Consultant, R&D
Vistorm Ltd
pgp://0xC563050C
pstn://+447973216090/is/robert/there?

[Back to top](#)



Display posts from previous:

[NewTopic](#)

[Reply to topic](#)

[PGP Forum Forum Index -> Certified PGP Engineers](#)

All times are GMT + 2 Hours

Page 1 of 1

[Stop watching this topic](#)

Jump to:



You **can** post new topics in this forum
You **can** reply to topics in this forum
You **can** edit your posts in this forum
You **can** delete your posts in this forum
You **can** vote in polls in this forum
You **can** [moderate this forum](#)