Good security practice for a Free Software release (DRAFT)

Alexandre Dulaunoy <adulau@foo.be>

14th August 2003

As you should already know, there is an excellent HOWTO[1] describing the good practice in software release done by Eric Raymond. But there are some additional good pratice to do in order to limit the risks of being corrupted, mangled or trojaned[2] when we are distributing our software. This document is created in order to keep a check list of good security practice for the Free Software developer during the distribution process. This document is ONLY focusing on software distribution.

0.1 Provide checksum of your files distribution

You should compute a message digest of your file distribution. You should use a strong digest algorithm like MD5 or better SHA1. Any recent Free Operating System like GNU/Linux includes software to generate digest from a file : md5sum or sha1sum (part of gnu-textutils). Here is an example :

```
[adulau@hydra adulau]$ md5sum foobar-1.2.3.tar.gz
bce9c4d6dcbfc3d069707c5b71d1fd5a  foobar-1.2.3.tar.gz
```

You should include the output in your software announce and in the file distribution directory. This is not enough to guarantee the integrity of your software packages. If your distribution site is compromised, the attacker could easily replace your file checksum with another one. To prevent that the software announce including the checksum helps but it's not enough. You should use OpenPGP as described after.

0.2 Make an OpenPGP signature of your files

At first, you should read the GnuPG[3] manual and understand the usage of GnuPG and the associated concept around OpenPGP. You (or the team of developers) have to create a pair of key for the software distribution or use your personal key (depending of the size and nature of your software project). To sign your file distribution you have multiple possibilities, here is some :

- You can make a clear-sign of the checksum file containing the information about your software distribution.

[1] http://www.ibiblio.org/pub/Linux/docs/HOWTO/other-formats/html_single/Software-Release-Practice-HOWTO.html

[2] http://foldoc.doc.ic.ac.uk/foldoc/foldoc.cgi?query=trojan&action=Search

[3] http://www.gnupg.org/

The clear-sign is a specific format of signature in OpenPGP for a text file. Here is a possible way of operation for signing your checksum file (we assume that you have correctly setup gnupg) :

```
[adulau@hydra gpg-test]$ ls -la
total 212
drwxrwxr-x    2 adulau   adulau       4096 Nov 14 16:13 .
drwx------   80 adulau   adulau      12288 Nov 14 16:13 ..
-rw-rw-r--    1 adulau   adulau     193903 Nov 14 16:13 foobar-1.2.3.tar.gz
[adulau@hydra gpg-test]$ md5sum * >MD5
[adulau@hydra gpg-test]$ cat MD5
bce9c4d6dcbfc3d069707c5b71d1fd5a  foobar-1.2.3.tar.gz
[adulau@hydra gpg-test]$ gpg --clearsign MD5
You need a passphrase to unlock the secret key for user:
"Alexandre Dulaunoy <alexandre.dulaunoy@ael.be>" 1024-bit DSA key, ID 44E6CBCD, created 2002-03-09
a passphrase was typed
[adulau@hydra gpg-test]$ ls
foobar-1.2.3.tar.gz  MD5  MD5.asc
[adulau@hydra gpg-test]$ cat MD5.asc
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1
bce9c4d6dcbfc3d069707c5b71d1fd5a  foobar-1.2.3.tar.gz
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.2.1 (GNU/Linux)
Comment: a comment for foobar distribution
iD8DBQE9073RCeLNSUTmy80RAgHQAJoDcBT1PtnrN595ArR3I/+tKmH62gCcDydY
ovnzF0HDCujvJ/CWl43QZ3c=
=SQp1
-----END PGP SIGNATURE-----
```

So now, you can include the signed MD5.asc file in your distribution site. Now everybody can verify your signature by doing a “gpg MD5.asc”. Don’t forget to add the checksum with the signature in your announce of a new release.

- You can make a detached signature of your files.

  The detached signature is the classical OpenPGP signature detached of the source file. Here is an example of doing a detached signature :

```
[adulau@hydra gpg-test]$ gpg --detach-sign foobar-1.2.3.tar.gz
a passphrase was typed
[adulau@hydra gpg-test]$ ls -la
total 224
drwxrwxr-x    2 adulau   adulau       4096 Nov 14 17:42 .
drwx------   80 adulau   adulau      12288 Nov 14 17:29 ..
-rw-rw-r--    1 adulau   adulau     193903 Nov 14 16:13 foobar-1.2.3.tar.gz
-rw-rw-r--    1 adulau   adulau         65 Nov 14 17:42 foobar-1.2.3.tar.gz.sig
```

So now, you can include the signature in your distribution site with your foobar-1.2.3.tar.gz. Everybody can now verify if the signature is correct with a “gpg foobar-1.2.3.tar.gz.sig”.

After that, you have to distribute the information about the signature via multiple channel (mailing-list, newsgroup, web site,...) in order to enhance the visibility of your public key and the corresponding checksum for a specific distribution.

0.3 Free Software announce

Here is an example of announce that can be used to inform the release of a new software package (including signature and checksum of the distributions file), the announce has also been clear-sign :

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

Hello,
We are please to announce the availability of a new release of foobar-1.2.3.
The files are available at the usual location :

ftp://ftp.foobar.org/pub/foobar-1.2.3.tar.gz
ftp://ftp.foobar.org/pub/foobar-1.2.3.tar.gz.sig

Please don't forget to check the integrity of the package;
either by verifying the provided OpenPGP signature (.sig)
or by comparing the  MD5 checksum:

bce9c4d6dcbfc3d069707c5b71d1fd5a  foobar-1.2.3.tar.gz

Thanks

The Foobar team.

-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.2.1 (GNU/Linux)
Comment: A foobar comment
iD8DBQE909gvCeLNSUTmy80RAvzbAJ4jdJdZfROOakRVFZ2SThbskKjHbQCfZ+Q2
q5dKWfPRY9RpRuHxXGNjoUs=
=pVAq
-----END PGP SIGNATURE-----
```

0.4 Be part of the OpenPGP web-of-trust

The most important part in OpenPGP is the web-of-trust. We will not in deep detail about web-of-trust in this document but if you want more information you should read the key management part of the GNU Privacy Guard manual.

So as a Free Software developer, you are encouraged to participate to key signing parties. There is a mailing-list for the information about the key signing parties coordination : http://lists.alt.org/mailman/listinfo/keysignings and there is also some web site to arrange key signing meeting : http://www.biglumber.com/