Verifying Apache Fineract Releases

由 Shaik Nazeer Hussain创建, 最后修改于一月 16, 2017

All official releases of code distributed by the Apache Fineract Project are signed by the release manager for the release. PGP signatures and MD5 hashes are available along with the distribution.You should download the PGP signatures and MD5 hashes directly from the Apache Software Foundation rather than from mirrors. This is to help ensure the integrity of the signature files. However, you are encouraged to download the releases from our mirrors.

Checking Signature

The following example details how signature interaction works. In this example, you are already assumed to have downloaded apache-fineract-0.6.0-incubating-src.tar.gz (the source release) and `apache-fineract-0.6.0-incubating-src.tar.gz.asc` (the detached signature). **In this example we are assuming you are verifying Apache Fineract 0.6.0-incubating release.**

This example uses The GNU Privacy Guard. Any OpenPGP -compliant program should work successfully.

First, we will check the detached signature (`fineract-0.6.0-incubating-src.tar.gz.asc`) against our release (`apache-fineract-0.6.0-incubating-src.tar.gz`).

```
% gpg --verify fineract-0.6.0-incubating-src.tar.gz.asc apache-fineract-0.6.0-incubating-src.tar.gz
gpg: Signature made 12/07/16 16:33:37 India Standard Time using RSA key ID 0BB29444
gpg: Can't check signature: No public key
```

We don't have the release manager's public key (0BB29444) in our local system. You now need to retrieve the public key from a key server. One popular server is `pgpkeys.mit.edu` (which has a web interface). The public key servers are linked together, so you should be able to connect to any key server.

```
% gpg --keyserver pgpkeys.mit.edu --recv-key 0BB29444
gpg: requesting key 0BB29444 from HKP keyserver pgpkeys.mit.edu
gpg: trustdb created
gpg: key 0BB29444: public key "Shaik Nazeer Hussain (CODE SIGNING KEY) <nazeer1100126@apache.org>" imported
gpg: Total number processed: 1
gpg: imported: 1
```

Another way to retrieve the public key is from KEYS file which is available as part Apache Fineract Project (https://dist.apache.org/repos/dist/dev/incubator/fineract)

```
% gpg --import KEYS
gpg: key B983100D: public key "Adi Raju (CODE SIGNING KEY FOR APACHE FINERACT) <rajuan@apache.org>" imported
gpg: key 0CB6C40C: "Shaik Nazeer Hussain (CODE SIGNING KEY) <nazeer.shaik@confluxtechnologies.com>" not changed
gpg: key 0BB29444: public key "Shaik Nazeer Hussain (CODE SIGNING KEY) <nazeer1100126@apache.org>" imported
gpg: Total number processed: 3
gpg:               imported: 2  (RSA: 2)
gpg:              unchanged: 1
```

In this example, you have now received a public key for an entity known as 'Shaik Nazeer Hussain<nazeer1100126@apache.org>' However, you have no way of verifying this key was created by the person known as Shaik Nazeer Hussain. But, let's try to verify the release signature again.

```
% gpg --verify apache-fineract-0.6.0-incubating-src.tar.gz.asc apache-fineract-0.6.0-incubating-src.tar.gz
gpg: Signature made 12/07/16 16:33:37 India Standard Time using RSA key ID 0BB29444
gpg: Good signature from "Shaik Nazeer Hussain (CODE SIGNING KEY) <nazeer1100126@apache.org>" [unknown]
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: AF4F D65D E78C A5B1 BF30  939F 80C4 D889 0BB2 9444
```

Let's verify binary release also. Download apache-fineract-0.6.0-incubating-binary.tar.gz (binary release) and its detached signature apache-fineract-0.6.0-incubating-binary.tar.gz.asc

```
% gpg --verify apache-fineract-0.6.0-incubating-binary.tar.gz.asc apache-fineract-0.6.0-incubating-binary.tar.gz
  gpg: Signature made 12/07/16 16:33:37 India Standard Time using RSA key ID 0BB29444
  gpg: Good signature from "Shaik Nazeer Hussain (CODE SIGNING KEY) <nazeer1100126@apache.org>" [unknown]
  gpg: WARNING: This key is not certified with a trusted signature!
  gpg: There is no indication that the signature belongs to the owner.
  Primary key fingerprint: AF4F D65D E78C A5B1 BF30 939F 80C4 D889 0BB2 9444
```

At this point, the signature(s) are good, but we don't trust this key. A good signature means that the file has not been tampered. However, due to the nature of public key cryptography, you need to additionally verify that key 0BB29444 was created by the **real** Shaik Nazeer Hussain.

Any attacker can create a public key and upload it to the public key servers. They can then create a malicious release signed by this fake key. Then, if you tried to verify the signature of this corrupt release, it would succeed because the key was not the 'real' key. Therefore, you need to validate the authenticity of this key.

Validating Authenticity of a key

You may download public keys for the Apache Fineract release managers from our website or retrieve them off the public PGP key servers (see above). However, importing these keys is not enough to verify the integrity of the signatures. If a release verifies as good, you need to validate that the key was created by an official representative of the Apache Fineract Project.

The crucial step to validation is to confirm the key fingerprint of the public key.

```
% gpg --fingerprint 0BB29444
pub   4096R/0BB29444 2016-06-29
      Key fingerprint = AF4F D65D E78C A5B1 BF30  939F 80C4 D889 0BB2 9444
uid       [ unknown] Shaik Nazeer Hussain (CODE SIGNING KEY) <nazeer1100126@apache.org>
sub   4096R/F11A0D70 2016-06-29
```

Checksum verification

Download apache-fineract-0.6.0-incubating-src.tar.gz.md5, apache-fineract-0.6.0-incubating-src.sha512, apache-fineract-0.6.0-incubating-binary.tar.gz.md5, apache-fineract-0.6.0-incubating-binary.sha512 files from https://dist.apache.org/repos/dist/dev/incubator/fineract/0.6.0-incubating/

The content of the file apache-fineract-0.6.0-incubating-src.tar.gz.md5 should be equal to the output of the following command

```
% gpg --print-md MD5 apache-fineract-0.6.0-incubating-src.tar.gz
  apache-fineract-0.6.0-incubating-src.tar.gz:
  53 BD 68 9E 41 DA 8D 34  80 70 CE 97 36 44 DF BE
```

The content of the file apache-fineract-0.6.0-incubating-binary.tar.gz.md5 should be equal to the output of the following command

```
% gpg --print-md MD5 apache-fineract-0.6.0-incubating-binary.tar.gz.md5
  apache-fineract-0.6.0-incubating-binary.tar.gz:
  10 D4 06 DC 4E 3A 53 32  F6 14 F9 42 E3 8C 65 F1
```

The content of the file apache-fineract-0.6.0-incubating-src.sha512 should be equal to the output of the following command

```
% gpg --print-md SHA512 apache-fineract-0.6.0-incubating-src.tar.gz
  apache-fineract-0.6.0-incubating-src.tar.gz:
  1AC9FEC6 781F6BD7 B14481A2 367E3BD2 049ECF5B 8EC3E1AB 675E02DE CC15FC6A DC0E1460 DD932023 CB1994BD F49738A2 A0A743CE 55
```

The content of the file apache-fineract-0.6.0-incubating-binary.sha512 should be equal to the output of the following command

```
% gpg --print-md SHA512 apache-fineract-0.6.0-incubating-binary.tar.gz
  apache-fineract-0.6.0-incubating-binary.tar.gz:
  D7FC2DF9 081A37B0 35F862EE 4D7D7A9A 86A97BA7 BE38BA80 71EA1D02 7116DA2C 1E6E11AD
  FDEAC129 C007F08E 7B397D4D 77D22E91 675E78F1 FF60C41A E891F058
```

无标签