Design and Analyze Secure Networked Systems 4

Prof. Edward Chow @ Colorado Univ.

Note by waegaein@github.com

Software Signing

- Provide ways to verify authenticity and integrity of software which are distributed via web.

- GPG

GNU Privacy Guard (GnuPG or GPG) is a tool for secure communication. It can be used to generate public/private key pair.

- PGP

Pretty Good Privacy (PGP) is encryption program that follows OpenPGP standard for encyption/decryption of data.

Sign Software

1. Finish a version for release.
2. Generate MD5 and SHA1 message digest of the software.
3. Generate PGP signature of the digest, using private key.
4. Distribute the software with the signature.

Verify Software

1. Download software and its signature.
2. Retrieve public key from key server.
3. Decrypt the signature into a digest.
4. Generate a digest by hashing the software.
5. If the two digests are identical, the software is verified.
6. If different, the software or signature is considered to be altered.

Mirror Sites

- Distribute software releases of other organizations to provide faster access.
- Not managed by the original author organizations.
- Encouraged to download bundle from mirrors.
- Discouraged to download hash and signatures only from the original.