

Security

Assignment 9, Wednesday 26 November, 2008

Goals: After successfully completing this exercise you should have a working grasp of digital signatures, and you should be able to send and receive encrypted and signed messages.

Deadline: Friday December 5 or earlier, send to Flavio's e-mail box (see the task itself).

1.
 - Find out how PGP (Pretty Good Privacy) works.
 - Generate a PGP-identity, and submit it at a public key server like <http://pgp.mit.edu> or <http://gpg-keyserver.de>.
 - Sign the key of at least one other student, and convince at least one other student to sign your key *on the server*.

For example, visit <http://www.cs.ru.nl/F.Garcia/> to see Flavio's PGP public key ID: 0xBCA32306 and experiment with <http://gpg-keyserver.de>.

2. Now you have a PGP-identity and you can use it to email securely. A convenient way to do this is via a plugin for your email-client, for example Enigmail for Mozilla Thunderbird.

Send an encrypted and signed ("a digital signature") email with the subject "Assignment 8 Security" to F.Garcia@cs.ru.nl, containing

- your name,
- your public key ID,
- indicate, which key is used for encryption and which for signing,
- finally, indicate in a few lines which security goal(s) you have achieved by sending this email.

(Take care: if you (accidentally) send us your *private* key, we will abuse it! >: -))