6^{th} Assignment Information Security

Francesco Segala 3521885 Manos Gionanidis 3542068

October 24, 2017

Excercise 34

I computed my gpg keypair with the linux built-in program gpg2. I followed the step that the prompt required and I come up with this fingerprint (the default setting generate a 2048 bit key using RSA algorithm):

```
/home/cesco/.gnupg/pubring.kbx
------------------------------
pub   rsa2048/E8168125 2017-10-21 [SC]
    Key fingerprint = B5D4 6CF5 839F 9EEC 7C1F  5A3E
        08E2 0B66 E816 8125
uid          [ultimate] Francesco Segala <francesco.
   segala10@gmail.com>
sub   rsa2048/E1D88B61 2017-10-21 [E]
```

Excercise 38

0.1 Question 1

Using GPG is preferable over the simple mail exchange because in sending email via simple MTAs that uses TLS encrypted means of transport there is no encryption between the sender and the MTA and also there is no encryption between the MTA and the receiver. So there are 2 opportunities to intercept the message, while using gpg ensure that the message that leaves and reach the clients is additionaly encrypted before leaving host machines and before reaching the target host. As before there is still encryption between the MTAs, so the MTAs encrypt the encrypted message during his route.Because Sendmail with TLS only can authenticate at the server level, true end-to-end authentication of the mail message cannot be performed with only the use of Sendmail Secure Switch. By including the use of S/MIME or PGP e-mail and trustworthy key hierarchies, full confidentiality and integrity can be accomplished from end-to-end of the mail message path.

0.2 Question 2

We sent an email to gionanide@csd.auth.gr email address using the sendmail command line, we setted up the configuration files in order to be able to send a TSL protected mail and , to the other hand we monitored the traffic with tcpdump tool listening on port 25. Following we post the commands we used:

```
$$ sendmail gionanide@csd.auth.gr
Subject : TEST EMAIL
Hello Manos
```

For sending the email and :

```
  sudo tcpdump -vv -x -X -s 1500 -i enp7s0 port 25 -
     w out.txt
```

Redirecting the output on the out.txt file. Scanning the file we cannot find anyone of the information in plaintext because either the body and the subject and all information are encrypted.

0.3 Question 3

To prevent that an intruder that gain acces to my computer read personal and confidential documents I would encrypt them with my public key so even if he can get them he is not able to read them without the secret passphrase. In fact even if he get the secret key file he cannot decrypt the files without inserting the passhprase.

0.3.1 Quesion 4

An example of information that we consider personal and confidential is : Private photos , passwords files, emails, daily schedule or diary.