Computer science, stationary program, graduate studies. Term II

Security of Information Systems **2016/2017**

Instructor: Ph.D. Eng. Rafał Grzybowski Tuesday, 12:15

Issue date: _____ Mark: _____

Michał Sośnicki 207597
Daniel Pęczek 207585

Secure file transfer - Practical part

1. Purpose

The purpose of this workshop is to show our implementation of secure file transfer mechanism for given security problem. We have chosen problem and technology to present how we could provide someone secure solution for file transmission. We decided to resolve problem of secure sending messages via email between two people and we wanted to use GNU Privacy Guard which is free implementation od OpenPGP standard which assure about secure file transfer when users follows simple rules of use it.

2. Problem statement

Our problem is to assure two ladies: Annie and Betty that information that they sending between two departments in different locations are properly secure from Mallory. Mallory is term used in cryptography and mean any person who wants to read transmitted files. In our problem we have to focus on three principles:

— Confidentiality Principle - Annie must be sure that informations sent and received from Betty cannot be read by Mallory.
— Integrity Principle - informations sent by ladies can't be modified in any way by Mallory.
— Nonrepudiation Principle - Betty must be sure that message that she received was send from Annie and Annie must be sure that recipient of message is Betty. Mallory can't impersonate for our ladies.

2.1. General

To provide secure file transfer we decided to use PGP mechanism which one of it implementations is available in GNU Privacy Guard.

2.2. GNU Privacy Guard

GNU Privacy Guard (or GnuPG) is a free implementation of PGP standard which offers all of standard core functionalities. GnuPG provide data encryption mechanism and user key generation and allow for digital signature to all sent data.
Recalling our three principles from earlier section that's how GnuPG is providing security:
— Confidentiality Principle - when Annie want to send data GnuPG is generating symmetric session key and encrypt data which are mean to send. Next symmetric key is asymmetric encyrpted with Betty public key. Encrypted message and session key is send to Betty. When Betty wants to read message she has to decrypt session key with her private key and after it she can decrypt message with received session key. This mechanism is simple and encryption and decryption process is done automatically without Annie or Betty interference.
— Integrity and Nonrepudation Principles - are resolved by the same GnuPG feature - digital signing. When Annie is sending data, hash for this data is

generated. Hash is also encrypted with Annie private key and attached to message. When Betty receive it she decrypt hash with Annie public key, then she compare decrypted hash value with hash of received message. If hash is correct, she is assure that nothing was modified and message was really sent from Annie.

3. Implementation

4. Results

Hello

Listing 1. Fragment

```
export A=”Dupa”
echo ”Dupa $A”
```

5. Review

6. Bibliography

— Michael W. Lucas, PGP & GPGEmail for the Practical Paranoid