GPG Practise

Wouter Borremans

October 17, 2004

1 Preface

This document describes the findings and answers regarding de GPG practise of the ESA subject.

2 Assignment 1

This assignment consisted of creating an installation of GnuPG. A part of this installation was to generate a pair of keys and publish them. First i downloaded the GnuPG program at www.gnupg.org. After that i began installing it;

- Unpack tarball with "tar -zxvf gnupg-1.2.6.tar.gz"
- Preperations for compiling; ".configure" followed by "make" and "make install"

After the installation i had to generate a pair of keys which i will use sending PGP encoded email;

- To start making a keypair, i used: "gnu –gen-key"

  algorithm: DSA and ElGamal (default)

  keysize: 1024 bit

  period for the key to be valid: 2w

  Real name: Wouter Borremans

  email address: wouter@wouter.os3.nl

  passphrase: password

  Now, to be able to use the key you need to publish it;

- The command to publish: "gpg - -keyserver pgp.met.edu - -send-keys wouter@wouter.os3.nl"

My public key is now published and can be used to send to someone.

3 Assignment 2

In this assignment i tested my keys using it with the text-based email client"Pine". In the pine program a few parameters (sending-filters)had to be send to integrate the GPG module. I used my own key to send my emails, to be able to send encrypted mails (e.g. to Maarten or Thijs) i first had to import their public keys. These keys can be imported using the following command;

- Search for keys which have a os3.nl address; "gpg - -keyserver pgp.mit.edu - -search-keys os3.nl"

The above command will query the key database and will return the addresses. You can select which keys to import.

To trust eachother using a SSH keypair;

- ssh-keygen -t rsa -f homewouterssh$_key$ This key needs to be send to the user you want to trust, this user must add this key to a specific user directory at his / her server in a file called "authorized_hosts". The user also needs to do that in the main ssh directory to be able to have passwordless access.

4 Assignment 3

In this assignment we had to be able to start remote X applications.

- Edit the SSH configuration and enable "X11Forwarding"

The SSH daemon needs to be restarted to activate the new configuration.

5 Assignment 5

A backup script can be created by executing a script that creates a tar-ball of specific user directory's. The cron daemon could look like;

```
# for vixie cron
#
# $Header: /var/cvsroot/gentoo-x86/sys-apps/vixie-cron/files/crontab-3.0.1-r4,v 1.6
#
#

# Global variables
SHELL=/bin/bash
PATH=/sbin:/bin:/usr/sbin:/usr/bin
MAILTO=root
```

```
HOME=/

# check scripts in cron.hourly, cron.daily, cron.weekly and cron.monthly
0  *  * * *     root    rm -f /var/spool/cron/lastrun/cron.hourly
1  3  * * *     root    rm -f /var/spool/cron/lastrun/cron.daily
15 4  * * 6     root    rm -f /var/spool/cron/lastrun/cron.weekly
30 5  1 * *     root    rm -f /var/spool/cron/lastrun/cron.monthly
*/10  *  * * *  root    test -x /usr/sbin/run-crons && /usr/sbin/run-crons

# Backup script
0 5 * * * root /scripts/backup > /dev/null
```