Посібник по GPG “на швидку руку”

Зміст

Це — переклад опублікованого в поштовій розсилці TLUG (Tokyo Linux Users Group) посібника за авторством Джонатана Байрн'а (Jonathan Byrne). В ориґіналі посібник названий «Quick-n-Dirty Guide to GPG>". Українською це перекладено як «Посібник по GPG на швидку руку». Відповідно абревіатура QND (від Quick-N-Dirty) передається НШР.

Переклав: Дмитро Ковальов, 2002 рік, Токіо

Ласкаво просимо до Посібника по GPG на швидку руку.

Посібники типу НШР мають велику кількість інформації типу «що"і зовсім мало типу "чому". Тому дуже корисною буде ознайомлення з інформацією на http://www.gnupg.org/docs.html.

Цей документ складається з семи секцій, які висвітлюють такі теми: як пересвідчитись, чи Ви маєте GPG встановлений, і чи встановлений вірно,

створення пари ключів, створення сертифікату для відкликання свого ключа, як працювати з серверами ключів і як повідомити стороннім про свій ключ.

Цей посібник НШР в його сьогоденній редакції орієнтований на дистрибутив, що базується на RPM, але в майбутньому будуть включені також інструкції для інших дистрибутивів і, можливо, будуть створені специфічні для кожного комплекту гілки.

Це — чорновий документ і зауваження та доповнення до нього приймаються.

Перш, ніж ви почнете

Прочитайте цього посібника від початку до кінця, перш, ніж починати робити будь-що. Після закінчення читання, переходьте до Розділу 1.

Частина I

Чи у Вас встановлений GPG?

В командній оболонці надрукуйте:

```
# which gpg
#
```

Ця команда повинна повернути командну доріжку до gpg, можливо `/usr/bin/gpg`.

Якщо команда знайде gpg, переходьте до розділу II. Якщо ні — продовжуйте далі з цим.

Якщо Ви продовжуєте читати, це означає, що Ваша система не відшукала gpg, коли Ви надрукували `which gpg`. В такому випадку Вам потрібно буде звантажити пакет GPG з сервера FTP Вашого дистибутива чи з його дзеркала.

Після того, як з вивантаженням закінчено, станьте адміністратором (su в користувача root) в командній оболонці, перейдіть в каталог, де у Вас встановлений RPM і надрукуйте:

```
# rpm -Uvh „назва-rpm"
#
```

Після цього команда `which gpg` повинна показати Вам, де знаходиться команда (можливо в `/usr/bin/gpg`).

Частина II

Встановіть GPG із SUID ROOT

Якщо у Вас немає доступу до адміністрування Вашої системи, можете пропутсити цей розділ.

Станьте адміністратором (root) і надрукуйте:

```
# chmod +s /path/to/gpg/from/step1/gpg
#
```

```
# chmod +s /usr/bin/gpg
#
```

Цей крок потрібен для того, щоб змусити GPG користуватись безпечними областями пам'яті.

Можете вийти з адміністративного рахунку в свій власний.

Частина III

Створіть пару ключів

Надрукуйте:

```
# gpg −−gen−key
#
```

Якщо Ви ніколи не створювали пару ключів до цього, Ви побачите таке:

```
gpg (GnuPG) 1.0.6; Copyright (C) 2001 Free Software Foundation, Inc.
This program comes with ABSOLUTELY NO WARRANTY.
This is free software, and you are welcome to redistribute it
under certain conditions. See the file COPYING for details.

gpg: /home/newbie/.gnupg: directory created
gpg: /home/newbie/.gnupg/options: new options file created
gpg: you have to start GnuPG again, so it can read the new options file
```

Це — нормальний вивід команди. Зараз ми ще раз повторимо її:

```
# gpg −−gen-key
#
```

1. Прийміть запропоноване значення для типу ключа (просто натисніть enter)
2. Введіть 2048 у відповідь на запитання про розмір ключа.
3. Вас спитають, чи справді Вам це потрібно. Так.

4. Вас знову спитають, про те, скільки часу Ви хотіли б щоб ключ діяв. Введіть 0 (стандартне значення).

5. Вас спитають, чи це вірно . Так.

Розділ налаштування імені користувача

1. Введіть ім'я і прізвище

2. Введіть поштову адресу (електронна пошта).

3. Додатковий коментар. Залиште пустим.

4. Підтвердіть ім'я, яке Ви ввели. Натисніть Enter(OK), якщо все в порядку.

Ваш ідентифікатор це Ваше ім'я + поштова адреса + додатковий коментар. Подібно до рядка поданого далі:

```
Ima Newbie (This is my comment) <imanewbie@imanewbie.com>
```

Важливе зауваження: наступний розділ присвячений паролю. Давайте почнемо з підрозділу з заголовком:

<DANGER>
Пароль — дуже важливий. Це має бути щось довге (речення а не слово) і містити в собі як великі, так і малі літери разом з розділовими знаками та цифрами. Зміна слів, за рахунок включення до них літер — часто гарна справа. Наприклад: 3 замість E/e, 4 замість A/a, 0 замість O/o, 1 замість L/l, 7 замість T/t, тощо. Це — стиль, яким користуються 31337 H4x0rs. Якщо Ви зрозуміли ці два слова — Ви на вірному шляху.
НЕ ЗБЕРІГАЙТЕ пароль на комп'ютері. НІКОЛИ. Зберігайте його поза мережею в безпечному місці. Приклеєний листочок до дисплея, чи листочок який лежить поруч з комп'ютером не відносяться до безпечних місць. Якщо можете запам'ятати цю фразу — це найкраще.
Відносьтесь до свого пароля серйозніше, ніж до пароля користувача root. Це — справді так.
</DANGER>

Тепер займемся створення пари ключів. Вас попросять зайнятись якоюсь іншою справою поки це робиться — повозити мишкою по столі чи подрукувати на клавіатурі. Це потрібно для створення надійного потоку випадкових даних. Починайте це робити зразу-ж. Ґенерація ключів займе не більше кількох секунд.

Частина IV

Створення сертифіката для відкликання ключа

Вам буде потрібен такий сертифікат на той випадок, якщо будь-коли Ваші ключі буде скомпроментовано (викрито) чи Ви згубите пароль. Зробіть це зараз — якщо Ви будете чекати доки це трапиться, буде вже занадто пізно. Ви не зможете цього зробити.

Надрукуйте:

```
# gpg ––gen-revoke "ВАШ-ІДЕНТИФІКАТОР"
#
```

Ваш ідентифікатор це Ваше ім'я + поштова адреса + додатковий коментар. Подібно до рядка поданого далі:

```
Ima Newbie (This is my comment) <imanewbie@imanewbie.com>
```

Приклад:

```
gpg $--$gen-revoke "Ima Newbie <imanewbie@imanewbie.com>"
```

Цей ґенератор сертифіката відкликання переспитає Вам такі речі (відповіді дані зразу ж за запитаннями):

1. Створити сертифікат відкликання (Create a recovation certificate?) y
2. Вкажіть причину (Select reason) : 2

3. Додатковий опис (Optional description): залиште пустим
4. Все вірно (Is this OK) ? y
5. Введіть пароль (Enter passphrase) : ВАШ-ПАРОЛЬ

На екрані Ви побачите свій сертифікат. Він буде подібним до чогось такого як:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.0.6 (GNU/Linux)
Comment: For info see http://www.gnupg.org
Comment: A revocation certificate should follow

<якийсь закодований текст в цьому місці>

-----END PGP PUBLIC KEY BLOCK-----
```

Виділіть цей текст і збережіть його де-небудь (дискета чи компакт-диск, тощо) або надрукуйте його. Компакт-диск краще, оскільки дискети не такі надійні. Обоє — друк і запис на компакт диск, мабуть найкращий варіант. Не зберігайте сертифікат відкликання на своєму комп'ютері, ніколи. З тої ж самої причини, з якої Вам не варто зберігати свій пароль на комп'ютері. Зберігайте його в надійному, безпечному місці, так само як і пароль.

Частина V

Надішліть свій відкритий ключ на сервер ключів

```
# cd  /.gnupg
#
```

Друкуйте:

```
# gpg --list-keys
#
```

Ви побачити щось типу:

```
pub  1024D/DF12B4EF 2002-07-27 Jonathan Byrne <bteam@gol.com>
```

Але в Вашому випадку тут буде йти Ваша інформація. Частина, яка Вам потрібна йде після pub 1024D/ (для мене це — DF12B4EF). Це — ідентифікатор мого ключа.

Під'єднайтесь до мережі, і після цього надрукуйте цю команду, підставивши свій ідентифікатор:

```
# gpg --keyserver pgp.mit.edu --send-keys
ВАШ-ІДЕНТИФІКАТОР
#
```

Повторіть те-ж саме з іншим сервером:

```
# gpg --keyserver www.keyserver.net --send-keys
ВАШ-ІДЕНТИФІКАТОР
#
```

Частина VI

Отримайте мій відкритий ключ

```
# gpg --keyserver pgp.mit.edu --recv-keys DF12B4EF
```

```
#
```

Тепер Ви готові як для відсилання, так і для отримання закодованих за допомогою GPG листів чи листів з електронним підписом. Як це робити буде описано в іншому документі.

Частина VII

Як повідомити іншим про Ваш ключ

Найпростіший спосіб повідомити іншим про свій ключ — це вставити в файл підпису (.signature) щоб рядок з інформацією про ключ був включений в Ваші листи. Мій файл .signature має такі рядки:

```
GPG key: DF12B4EF (5399 C834 3ABB C3AF 610C  5345 D5D6 E6EA DF12 B4EF)
gpg --keyserver pgp.mit.edu --recv-keys  DF12B4EF
```

Два рядки з моїм ключем, «відбитком пальців» та командою для отримання ключів з сервера.