Pràctica 9: GnuPG

Aplicacions i serveis d'internet — iTIC

Francisco del Águila López Aleix Llusà Serra Alexis López Riera

10 de maig de 2013

Índex

Resum

Enviament de missatges segurs: GnuPG. Xifrat i Signatura de missatges. Relació de confiança: Autoritats de Certificació i Certificats.

1 Organització

1.1 Objectius

Els objectius d'aquesta pràctica són:

1. Entendre quins són els mecanismes d'intercanvi de missatges amb seguretat.
2. Conèixer els mecanismes de xifrat i signat de missatges.
3. Còneixer el paper que juguen les autoritats de certificació en l'intercanvi de missatges amb seguretat.
4. Entendre en què consisteix un certificat digital.
5. Utilitzar algoritmes de xifrat / signat.

1.2 Condicions

- La pràctica està calibrada per a ésser treballada en equips de dues persones.
- La durada de la pràctica és de 1 setmana.

1.3 Lliurables

Heu d'entregar:

- Un informe amb els missatges intercanviats segons les tasques descrites a la pràctica.

1.4 Material necessari

Per tal de fer servir una comunicació segura entre els missatges intercanviats, cal disposar de:

- L'aplicació `gpg` que forma part del paquet `gnupg`.

  TASCA PRÈVIA 1 Instal·leu el que us faci falta per realitzar aquesta pràctica, encara que en la majoria de distribucions aquest paquet ja ve preinstal·lat.

2 Xifrat de clau pública

En els mecanismes de clau pública, cada usuari ha de disposar d'un parell de claus. La clau pública és la que es difondrà. Amb aquesta clau pública, qualsevol pot enviar un missatge xifrat o bé comprovi la signatura d'un missatge signat. La clau privada es protegirà i s'utilitzarà tant per desxifrar els missatges dirigits cap a l'usuari com per generar un missatge signat.

Amb el `gnupg` es pot treballar plenament amb el sistema de xifrat de clau pública, per tant es pot:

- Generar el parell de claus.
- Gestionar un dipòsit de claus. Aquest dipòsit quedarà integrat en el sistema i es podrà fer us de les claus des de un conjunt d'aplicacions incloent l'entorn gràfic.
- Importar i explortar claus.
- Desxifrar missatges (usant la clau privada pròpia).
- Xifrar missatges (usant la claus pública de a qui se li envia el missatge).
- Signar missatges (usant la clau privada pròpia).

La documentació sobre el funcionament del `gpg` la podeu trobar a

- `man gpg`: hi ha la descripció exhaustiva de l'aplicació.
- `http://www.gnupg.org/documentation/howtos.en.html`: es troben tutorials d'aquesta aplicació.

3 Entorn de treball

Per treballar amb aquesta eina simularem un entorn de treball amb un canal de comunicació insegur. Aquest canal de comunicació consistirà en publicar tots els missatges a un fòrum d'Atenea. D'aquesta manera tothom podrà veure els missatges i per tant podran ser susceptibles de ser analitzats.

En aquest fòrum s'obrirà un debat per poder deixar les vostres claus públiques. Aquest és el mecanisme per difondre les claus i que estiguin disponibles per tothom. En el funcionament normal del `gnupg` existeix la possibilitat de publicar les claus públiques en una xarxa mundial de servidors que s'encarreguen de fer-les disponibles per a tothom `http://keys.gnupg.net/`.

La generació del parell de claus pot fer-se escollint diferents algoritmes. Per aquesta pràctica s'ha de vigilar que s'escolli un algoritme que permeti tant el signat com el xifrat sense cap tipus de restricció de patents o royalties.

> Tasca prèvia 2 Genereu el parell de claus (la pública i la privada). Comproveu que la clau privada queda suficientment protegida i difongueu la clau pública enviant un missatge al fòrum comunitari.

4 Mètode de treball

Quan es vulgui enviar un missatge a algú, es publicarà al fòrum. El missatge que s'envia al fòrum consistirà en:

1. Primera línia de text indica qui és el destinatari o destinataris del missatge.
2. Les següents línies consisteixen en el text xifrat i/o signat en format ASCII per facilitar la feina de còpia del missatge.

A continuació realitzeu el conjunt de tasques següents:

Tasca 3 Importeu les claus públiques tant del professor com de la resta de companys. Això permetrà que pugueu enviar missatges xifrats o comprovar les signatures.

Tasca 4 Respongueu al missatge enviat pel professor seguint les instruccions del propi missatge.

Tasca 5 Envieu un missatge signat al fòrum en text clar.

Tasca 6 Intercanvieu missatges entre vosaltres i comproveu el correcte funcionament del `gpg`.

Tasca 7 Si algú aconsegueix desxifrar o signar un missatge que no sigui dirigit/originat per a ell que ho manifesti i es tindrà molt en compte.