Seguridad de Sistemas Informáticos - práctica 6

GPG y X509

1. Utilizando el software gpg, generar un par de claves DSA-elGamal de 2048 bits. (`gpg --full-gen-key`), o aprovechar la utilizada en el práctico anterior.

2. Exportar la clave pública a un archivo (`gpg --armour --export <clave> --output <archivo>`)

3. Intercambiar la claves pública con un compañero e importarla.

4. Asignar nivel de confianza 4 (Full Trust) a la clave del compañero, y luego firmarla. (`gpg -edit-key <clave>` 'trust' 4 'sign'.

5. Exportar la clave pública del compañero y devolvérsela. Recibir la clave propia firmada por el compañero.

6. Revisar las firmas (`gpg -list-sigs <clave>`)

7. Repetir los pasos del 2 al 5 con un segundo compañero.

8. Recibir la clave pública de un tercer compañero, que esté firmada por alguno de los compañeros a quienes le dimos confianza en los pasos anteriores, y verificar el nivel de confianza que se posee sobre esa clave.

9. Subir todas las claves públicas a un servidor. (`gpg --keyserver hkp://keys.gnupg.net --keyserver-options no-self-sigs-only --send-key <identificador>`) si hay conexión disponible.

10. Preparar el espacio para una nueva autoridad certificante X509. En en el servidor, hacer una copia del directorio CAtest con su contenido. Si trabaja en su máquina pesonal, utilice los directorios por defecto que propone la distribución.

11. Editar los archivos CA.pl y openssl.cnf para ajustar los valores por defecto, directorios y ubicación de los archivos.

12. Crear la autoridad certificante con `./CA.pl -newca`, completando los datos del certificado de la misma.

13. Crear una solicitud de certificado para una dirección de correo: `./CA.pl -newreq`

14. La clave privada se encuentra en el archivo newkey.pem, y el requerimiento se encuentra en el archivo newreq.pem. Remover el cifrado simétrico de la clave privada (`openssl rsa -in newkey.pem -out key.pem`). Verificar los permisos del archivo key.pem: la máscara debería ser 0600 (`rw-------`) o 0640 (`rw-r-----`). En nignún caso debería tener permiso de lectura, escritura o ejecución para todos.

15. Intercambiar los archivos newreq.pem para que un compañero lo firme con su autoridad certificante y viceversa: `./CA.pl -sign`. Devolver el certificado firmado newcert.pem al compañero.

16. Renombrar newcert.pem a cert.pem. Junto con la parte privada (key.pem) se pueden utilizar en un servidor.

17. Juntar nuevamente cert.pem y key.pem para formar fullcert.pem. Cuidar los permisos del archivo fullcert.pem. (`touch fullcert.pem ; chmod 600 fullcert.pem ; cat cert.pem key.pem > fullcert.pem`).

18. Construir una verrsión pkcs12 del certificado (`openssl pkcs12 -export -in newcert.pem -out newcert.p12`) e importarlo en un navegador para su uso.