Práctica IV.: Criptografía y Protocolos Seguros

Prof. A. Santos del Riego
Protección y Seguridad de la Información (PSI)
Facultad de Informática. Universidade da Coruña

El objetivo de esta práctica es comprender la importancia de los algoritmos criptográficos y su aplicación-funcionamiento en la forma de protocolos seguros. Hemos tratado en las clases teóricas los conceptos que rigen el funcionamiento de los criptosistemas simétricos y asimétricos, así como su integración híbrida en protocolos seguros. Se ha estudiado el esquema de funcionamiento de la firma digital y la necesidad de autoridades certificadoras. Finalmente, se ha presentado el funcionamiento de algunos protocolos y entornos seguros (SSH, GPG, SSL, etc.). Se deberán aplicar los conceptos adquiridos en la resolución de los siguientes apartados:

1. Tomando como base de trabajo el GnuPG y utilizando dos usuarios de su máquina virtual pruebe sus diversas utilidades:
    a. Generación de pares de claves
    b. Cifrado y descifrado asimétrico de ficheros
    c. Cifrado y descifrado simétrico de ficheros
    d. Firma de ficheros
    e. Verificación de la firma
    f. Generación de ficheros de firma acompañante
    g. Intercambio de claves
    h. Validación de claves
    i. Revocación de claves
    j. Gestión básica de claves
2. Analice el proceso criptográfico que se realiza en cada uno de los subapartados del punto anterior.
3. Tomando como base de trabajo el SSH pruebe sus diversas utilidades:
    a. Abra un *shell* remoto sobre SSH y analice el proceso que se realiza. Configure su fichero `ssh_known_hosts` para dar soporte a la clave pública del servidor.
    b. Haga una copia remota de un fichero utilizando un algoritmo de cifrado determinado. Analice el proceso que se realiza.
    c. Exporte una sesión X de forma segura.
    d. Configure su cliente y servidor para permitir conexiones basadas en un esquema de autenticación de usuario de clave pública.
    e. Utilice el agente de soporte de claves como complemento al apartado anterior.
    f. Mediante túneles SSH securice algún servicio no seguro.
4. Tomando como base de trabajo el servidor Apache2
    a. Configure una Autoridad Certificadora en su equipo.
    b. Cree su propio certificado para ser firmado por la Autoridad Certificadora. Bueno, y fírmelo.
    c. Configure su Apache para que únicamente proporcione acceso a un determinado directorio del árbol web bajo la condición del uso de SSL y previa autenticación.
5. Tomando como base de trabajo el openVPN deberá configurar una VPN entre dos equipos virtuales del laboratorio que garanticen la confidencialidad entre sus comunicaciones.