PRÁCTICA 3: Protocolos

Seguridad de la Información
Curso 2018-2019

Lenguajes y Ciencias de la Computación.
E.T.S.I. Informática, Universidad de Málaga

RELACIÓN DE EJERCICIOS:

1. (**10 puntos**) Los ficheros n-s-a.py e n-s-t.py implementan los pasos 1 y 2 del protocolo Needham-Schroeder básico (ver transparencias del tema 3).

   Se pide lo siguiente:

   a. (**7.5 puntos**) Terminar la implementación del protocolo Needham-Schroeder básico, implementando los pasos 3-5 junto con un intercambio de datos donde Alice y Bob intercambien sus nombres a través del canal de información seguro. Para ellos los alumnos no solo deberán completar el fichero n-s-a.py, sino también crear un fichero n-s-b.py que contengan los pasos realizados por Bob.
   b. (**2.5 puntos**) Implementar el ataque 2 al protocolo Needham-Schroeder básico (ver transparencias del tema 3) de la siguiente forma:
      i. Modificar el programa n-s-a.py del apartado a), de tal forma que Alice guarde el mensaje $E_{BT}(K_{AB}$, Alice) en el disco duro.
      ii. Crear un programa n-s-m-py, que implemente el ataque 2. Para ello, Mallory (que conoce K_{BT}) leerá el mensaje $E_{BT}(K_{AB}$, Alice) del fichero, y realizará los pasos 3-5 del protocolo Needham-Schroeder junto con Bob. Al final, Mallory y Bob intercambiarán sus nombres a través del canal de información seguro.

En este ejercicio, se utilizará la clase SOCKET_SIMPLE_TCP del campus virtual, que permite crear un cliente y un servidor TCP básicos.