Práctica 2: DTLS

El protocolo TLS apareció como una estandarización del IETF a partir del protocolo SSL v3.0 (actualmente, la versión es TLS v1.1, publicada en la RFC 4346). Dada su popularidad y facilidad de integración, es el principal protocolo para establecer seguridad en el tráfico en red hoy en día, y se aplica a diversos protocolos como por ejemplo a HTTP, IMAP o POP. El problema de TLS es que requiere un canal de transporte fiable (como el proporcionado por TCP), y no puede ser utilizado para garantizar la seguridad en tráfico de datagramas, es decir, tráfico que utilice UDP como los protocolos DNS, RTP (Real Time Protocol) y numerosas aplicaciones como los juegos Quake y Starcraft.

En este escenario aparece el protocolo que en el que en esta práctica se pretende profundizar, Datagram Transport Layer Security (DTLS), el cuál puede consultarse en la RFC 4347. La idea principal tomada para el diseño de este nuevo protocolo es la de reutilizar al máximo el existente TLS, con el fin de reutilizar las aplicaciones y protocolos montados sobre él. DTLS tiene que lidiar con algunos de los problemas que en TLS no aparecen por la naturaleza de TCP, como son el establecimiento de la conexión, el mecanismo de retransmisiones en caso de pérdidas, la reordenación de los paquetes fragmentados, etc. Para ello, en los paquetes DTLS se han añadido algunos campos, como números de secuencia, cookies, etc. Lo primero que el alumno deberá hacer es localizar dichos campos. También aparece un nuevo subprotocolo, llamado HelloVerifyRequest, encaminado a evitar ataques de denegación de servicio (DoS).

Aunque para la implementación con JPCapDumper no es necesario tenerlo en cuenta, el alumno deberá estar también familiarizado con el proceso de temporización/retransimisión de los paquetes en caso de que se pierdan, ya que es una de las novedades del protocolo. Dicho proceso puede consultarse en la propia RFC.

Se proponen las tareas siguientes:

1. Analizar y estudiar la traza ofrecida atendiendo a las siguientes preguntas:
   - ¿Cuáles son los mecanismos ofrecidos por TCP para TLS y que no ofrece UDP para DTLS? ¿Cómo se resuelven en el nuevo protocolo?
   - ¿Qué diferencias existen entre los paquetes TLS y DTLS?
2. Realizar las ampliaciones necesarias al programa JpcapDumper para que sea capaz de identificar y mostrar la información relativa a los paquetes que incluyen información de DTLS y de cada uno de los subprotocolos que lo componen. (Se recomienda utilizar el WireShark como ejemplo).