Práctica 2: DTLS
OpenCourseWare

Seguridad en Sistemas Distribuidos

Índice

- TLS sobre UDP
- Estructura de TLS y DTLS
- Flujo de Mensajes
- Tarea a Realizar

TLS sobre UDP

- SSL/TLS es el protocolo más utilizado para la seguridad en red (RFC 4346)
- Montado sobre TCP.
- El auge de las aplicaciones y protocolos sobre UDP demandan un protocolo nuevo.
- DTLS nace con esta intención.
- Ciertos mecanismos de TCP deberán ser implementados en la capa de aplicación (es decir, por DTLS).

Estructura TLS

Cliente

Servidor TLS

TCP

TLS

Record Layer

Handshake

Change Cipher Spec

Alert

Application data

Client Hello

Server Hello

...

HTTPs

Correo

Estructura DTLS

Cliente

Servidor DTLS

UDP

DTLS

Record Layer

Handshake

Change Cipher Spec

Alert

Application data

Client Hello

Hello Verify Request

Server Hello

...

Quake

DNS

RTP

Flujo de Mensajes

ClientHello

HelloVerifyRequest

ClientHello

Server Hello
Certificate
ServerHelloDone

ClientKeyExchange
[ChangeCipherSpec]
Finished

[ChangeCipherSpec]
Finished

Application Data

Tarea a Realizar

- Entender y comprender DTLS
- Identificar las diferencias con TLS
- Modificar JpcapDumper para que:
  - Sea capaz de identificar y mostrar la información relativa a DTLS y sus subprotocolos
- Informe:
  - Descripción del protocolo
  - Diferencias con TLS
  - Análisis del protocolo
  - Detalles de implementación: Problemas, soluciones, etc.

Referencias

- RFC 4347 (DTLS)
- RFC 4346 (TLS)
- Safari Books
  - Disponible desde la Universidad y VPN
- Documentación Jpcap y JpcapDumper