Asignatura	Datos del alumno	Fecha
Seguridad en redes	Apellidos: Paz Lopez	24/06/2021
	Nombre: Angel Ramón	

MECANISMOS DE SEGURIDAD	
Cifrado	X
Firma digital	X
Control de acceso	☐
Integridad de datos	X
Intercambio de autentificación	X
Relleno de tráfico	X
Control de enrutamiento	☐
Notarización	☐
Funcionalidad fiable	☐
Etiquetas de seguridad	☐
Detección de acciones	☐
Informe para auditoría de seguridad	☐
Recuperación de la seguridad	☐

ANÁLISIS

CIFRADO: **ACTIVO**

Procedimiento mediante el cual haciendo uso de un algoritmo, se transforma un mensaje para que sea incomprensible para aquellas personas que no sepan la clave de cifrado y el algoritmo usado. Y mediante la arquitectura SSL nos proporciona autenticación, integridad y confidencialidad de la información en cada extremo de la comunicación a través de mecanismos criptográficos. Del Intercambio de Mensaje del protocolo HandShake Protocol (la cual el protocolo permite la autenticación de servidor y cliente, negocia el algoritmo de cifrado y entre otras actividades que protegen los datos) podemos analizar que en la en la Fase 1 vemos el inicio de la conexión y combinaciones de algoritmos con los mensajes Client Hello y Server Hello segunda fase entre los

más importantes para ver si cumple el mecanismo de cifrado el mensaje ServerKeyExchange lo cual es necesario para el intercambio de claves y en la tercera fase el mensaje ClientKeyExchange en la cual el cliente envía el cifrado el secreto maestro con la clave publica del servidor.

FIRMA DIGITAL: **ACTIVO**

Método criptográfico que asocia la identidad de una entidad a un mensaje y que permite al receptor verificar la identidad de la fuente y la integridad del mensaje. Según las fases del SSL tenemos que al momento de Autenticación del Servidor la cual se lleva acabo al inicio del protocolo por medio del envió de la clave pública del servidor, mediante el certificado x.509 que se envía al establecer la conexión junto con la firma digital. Y en la autenticación del Usuario, consiste en una firma digital generada por el usuario haciendo uso de la clave privada y del envío de su clave publica por medio del certificado x.509.

CONTROL DE ACCESO: **INACTIVO**

Permite realizar una separación de privilegios individual para cada identidad que pueda acceder a un sistema. Pero según el tráfico de datos del ejercicio el cliente no envía el certificado en la fase 3 por lo cual la conexión será de forma anónima.

INTEGRIDAD DE LOS DATOS: **ACTIVO**

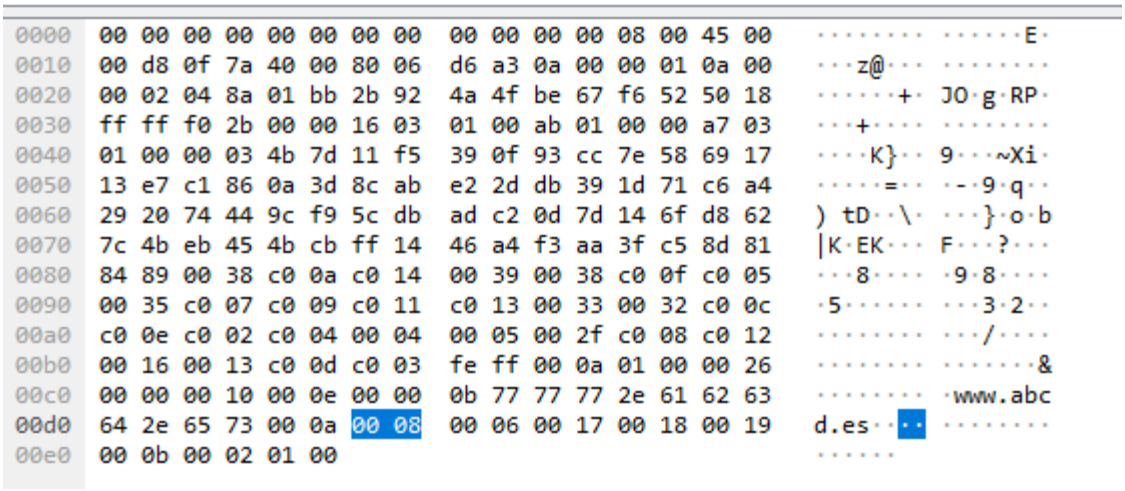
Mecanismo empleado para verificar la integridad de los mensajes intercambiados en una comunicación entre entidades. Activo porque Cumple porque con el protocolo Handshake Protocol además de permitir la autenticación del cliente y del servidor y de negociar el algoritmo de cifrado, calcula las claves para las MACS y las claves simétricas que se utilizaran para proteger los datos y mediante los mensajes ClientHello y ServerHello en la fase uno podemos revisar las listas de algoritmos de cifrado y de compresión en la segunda fase por parte del Servidor el Certificate (la cual da fe de la integridad) y el ServerKeyExchange lo cual requiere que el cliente se autentique, lo pasa a la fase 3 con el mensaje ClientExchange donde este envía cifrado los datos pertinentes y para finalizar vemos el mensaje ChangeCipherSpec donde el cliente pasa a utilizar los algoritmos y claves negociados.

INTERCAMBIO DE AUTENTICACION: **ACTIVO**

Mecanismo diseñado para verificar la identidad de un usuario o entidad a través de un intercambio de información. Activo porque en el intercambio de mensaje con el protocolo handshake en la fase 2 y en la fase 3 podemos ver los mensajes serverKeyExchange y clientKeyExchange en la cual el servidor requiere la autenticación del cliente para el intercambio de claves y el cliente envía cifrado sus datos correspondientes de manera cifrada

RELLENO DE TRAFICO: **ACTIVO**

Mecanismo que permite proteger el tráfico frente a posible análisis. El mensaje ClientHello inicia el protocolo TLS y la cual se compone de un encabezado especifico seguida de un encabezado, de algunas extensiones que son opcionales y seguidas de un relleno opcional.



CONTROL DE ENRUTAMIENTO: **INACTIVO**

Mecanismo que permite la selección de rutas seguras para el envió de determinados datos. En el trafico del ejercicio no se apreció ningún mecanismo de selección de rutas.

NOTARIZACION: **INACTIVO**

Mecanismo de Registro de Datos. No se apreció ninguna tercera entidad para el registro de Datos.

CUADRO COMPARATIVO SSL - IPSEC

SERVICIOS DE SEGURIDAD	SSL	IPSEC
Confidencialidad	La arquitectura SSL en si provee de confidencialidad a la información entre los extremos de la comunicación a través de mecanismos criptográficos, utilizando claves publicas para cifrar los datos. Además, provee servicios de autenticación a los extremos, aunque habitualmente solo el servidor es autenticado la cual hace que el medio o el canal de comunicación creado sea confidencial. También mediante el protocolo SSL Récord brinda el servicio de confidencialidad a partir del protocolo handshake que genera una clave secreta compartida, la cual es usada para cifrar los daros.	El estándar incorpora el servicio de confidencialidad de la comunicación haciendo uso de las Asociaciones de seguridad en la cual se establecen aspectos como los algoritmos de cifrado, además la Arquitectura de Seguridad IP considera dos nuevos protocolos y uno de ellos dota de confidencialidad a los datagramas IP de forma que la información que haya sido cifrada solo sea accesible solo para aquellas personas que estén autorizadas. Se recomienda AES ya que es el mejor en seguridad.
Autenticación	**Moderada** La arquitectura SSL provee de Autenticación en los extremos de la comunicación tanto para el servidor como para el usuario o cliente, la autenticación del servidor se lleva a cabo al inicio del protocolo (Handshake) por medio del certificado x.509 que se envía al no mas establecer la conexión, y la autenticación del usuario se lleva a cabo con la firma digital generada por el usuario haciendo uso de claves privadas y del envío de su clave publica por medio del certificado x.509, este es opcional ya que habitualmente solo el servidor es autenticado. El protocolo handshake es el que permite la autenticación del servidor y cliente.	**Segura** El estándar provee de autenticación mediante los protocolos AH (Cabecera de Autenticación) utiliza algoritmos de autenticación, proporciona integridad y autenticación a los datagramas IP, de forma que el receptor de un mensaje pueda detectar si este fue modificado o manipulado y si el autor es quien dice ser, ESP (Protocolo de Encapsulación Segura del campo de carga) también utiliza tanto algoritmos de cifrado como de autenticación.
Integridad	Como en los otros servicios la arquitectura SSL ya provee de Integridad de la información a partir de una clave que es generada en el handshake para generar una MAC y los demás procesos y fases que se realizan con los protocolos SSL Récord y SSL Handshake	Se implementa mediante algoritmos de HASH como SHA y MD5 y tanto los protocolos AH y ESP cuentan con los mecanismos de verificación y de protección de integridad en la transferencia de información.

No repudio	No hay ningún método que deje constancia de que se haya realizado ninguna operación en la comunicación, en este aspecto SSL falla por completo.	Es posible si se usa IKE con autenticación mediante certificados digitales, lo cual se basa en la firma digital de un mensaje que contiene y otros datos para identificar el usuario a quien corresponde dicho mensaje. Dicha firma gracias al vinculo entre las claves publicas y la identidad del usuario la cual garantiza el certificado digital, son prueba suficiente para comprobar de que se ha establecido una conexión IPSEC con un equipo determinado.

ANALISIS COMPARATIVO

La implementación de cada tecnología depende de las necesidades que presente la organización por la cual la organización puede implementar las dos a la misma vez. IPSEC trabaja en la capa de red y es la mejor opción en cuanto a Seguridad General y si se necesita mantener un acceso local permanente a una red privada fuera de la empresa, SSL trabaja en la capa de aplicación y es mejor opción en cuanto a soporte, facilidad de implementación y se necesite tener un control de acceso de usuarios remotos.

Podemos decir que IPSEC todas sus aplicaciones son basadas en IP, en cuanto a cifrado en mas segura ya que la longitud de sus claves son mayores (50 a 256 bits) que el SSL, en Autenticación es segura y bidireccional mediante certificados digitales, su acceso es de igual a igual mediante software, mientras SSL sus aplicaciones solo son basadas en la Web, en cifrado en comparación al IPSEC es Moderado a segura solo que las longitudes de sus claves son un poco más pequeñas (40 a 256 bits), su acceso es remoto y mediante al uso de un portal web.

Al comparar ambas tecnologías con lo investigado he llegado a la conclusión que la tecnología IPSEC supera a la tecnología SSL por los siguientes puntos:

- Las aplicaciones que admite
- Cifrado más seguro
- Autenticación sólida y más segura
- Seguridad en General

Además, que la tecnología SSL no cuenta con ningún método de No repudio que deje constancia de que se hayan realizado ninguna operación en la comunicación

REFERENCIAS

7.3.2.6 Marco del protocolo IPsec. (s. f.). Recuperado 18 de junio de 2021, de https://www.itesa.edu.mx/netacad/networks/course/module7/7.3.2.6/7.3.2.6.html

Algoritmos de autenticación y cifrado en IPsec (Guía de administración del sistema: Servicios IP). (s. f.). Oracle. Recuperado 18 de junio de 2021, de https://docs.oracle.com/cd/E19957-01/820-2981/ipsec-ov-11/index.html

Iglesias, S. P. (2001). *Análisis del protocolo IPSec: El estándar de seguridad en IP*. 14.

Comparando los protocolos IPSEC y SSL,¿Cual de los dos es mejor? (s. f.). Comunidad Huawei Enterprise. Recuperado 18 de junio de 2021, de https://forum.huawei.com/enterprise/es/comparando-los-protocolos-ipsec-y-ssl-%C2%BFcual-de-los-dos-es-mejor/thread/580384-100233

Moreno, L. (s. f.). *HTMLWeb. Seguridad. Secure socket Layer SSL (VII)*. Recuperado 18 de junio de 2021, de https://usuaris.tinet.cat/acl/html_web/seguridad/ssl/ssl_7.html

UNIR - TEMA 2—EL PROFESIONAL DE LA SEGURIDAD DE LA INFORMACIÓN. (s. f.). Recuperado 16 de junio de 2021, de https://micampus.unir.net/courses/17652/external_tools/95196

UNIR - TEMA 3—PROTOCOLOS DE SEGURIDAD. (s. f.). Recuperado 18 de junio de 2021, de https://micampus.unir.net/courses/17653/external_tools/95202

7.4.2.4 Comparación de IPsec y SSL. (s. f.). Recuperado 24 de junio de 2021, de https://www.itesa.edu.mx/netacad/networks/course/module7/7.4.2.4/7.4.2.4.html