EVALUACIÓN DE LOS PROTOCOLOS IPSEC Y SSL EN LA TRANSMISIÓN SEGURA DE IMÁGENES DIAGNOSTICAS EN TELERADIOLOGIA UTILIZANDO EL ESTÁNDAR DICOM

Jorge Luis Lugo Rosero
Ingeniero Electrónico de la Universidad Distrital Francisco José De Caldas, especialista en Teleinformática de la Universidad Distrital Francisco José de Caldas. Se desempeña como ingeniero de soporte en STID Ltda.
jorge.lugo@stidltda.com

Oscar Andrés Pérez Acuña
Ingeniero en Control Electrónico de la Universidad Distrital Francisco José de Caldas, especialista en Teleinformática de la Universidad Distrital Francisco José De Caldas. Se desempeña como ingeniero de soporte en el área de Sistemas del Hospital Infantil Universitario de San José en Bogotá.
anper81@gmail.com

Nancy Y. García
Ingeniera de Sistemas, MSc (c). en Ciencias de la Información y las Telecomunicaciones, docente de ingeniería de sistemas de la Escuela Colombiana de Carreras Industriales (ECCI).
ngelvezg@ecci.edu.co

Tipo: Artículo revisión de tema

Fecha de Recepción: Sept. 20 de 2010
Fecha de Aceptación: Marzo 15 de 2011

IPSEC-AND-SSL PROTOCOL EVALUATION FOR THE SECURE TRANSMISSION OF TELE-RADIOLOGY DIAGNOSIS IMAGES USING DICOM STANDARDS

Abstract
Digital diagnostic images are now a paradigm for the requirements of any computer system. Confidentiality of patient's medical information must be ensured through secure communications systems, thereby complying with the policies of quality control in Tele-radiology techniques. This paper first describes a typical communication scenario between plates-capture devices and the elements of visualization and storage. Then the manner in which the sampling diagnostic is transmitted from one place to another is presented. Additionally, the most commonly used protocols for this task are compared. A final discussion is provided on the results obtained when transmitting several medical studies on a LAN to ensure security and confidentiality of data.

Keywords: IPSec, SSL, DICOM, AES, DES.

Resumen
Las imágenes diagnosticas digitales constituyen hoy día un paradigma de requerimientos para cualquier sistema informático; se debe garantizar la confidencialidad de la información médica de los pacientes mediante sistemas de comunicación seguros, cumpliendo de esta manera con las políticas de control de calidad en técnicas de Tele-radiologia. En este articulo primero se describe un escenario típico de comunicación entre los dispositivos de captura de placas y los elementos de visualización y almacenamiento de las mismas, así como la forma en la que se transmiten dichas tomas diagnósticas de un sitio a otro, posteriormente se realiza la comparación entre los protocolos más utilizados en esta tarea y finalmente se analizan los resultados obtenidos al transmitir varios estudios médicos por una red LAN garantizando la seguridad y confidencialidad de los datos de trabajo.

Palabras clave: IPSec, SSL, DICOM, AES, DES.

1. INTRODUCCIÓN

En las últimas décadas el rápido desarrollo de las TICs ha abierto innumerables posibilidades para el intercambio de la información en materia de salud, haciendo posibles nuevas formas de asistencia, incluso las realizadas a distancia entre el profesional de la salud y el paciente.

En el contexto de las emergencias el principal problema es asegurar el tiempo de reacción para generar una ayuda adecuada, en este caso esta puede estar asociada al riesgo de muerte o secuelas graves. En este sentido hay que determinar los factores que puedan influir en la toma de decisiones sobre traslados y atención especializada. Ello hace necesaria la valoración del papel de la telemedicina en la puesta en marcha de todos los dispositivos implicados en el diagnóstico y tratamiento de las urgencias médicas. Por ello es vital la importancia del manejo de las comunicaciones en el ámbito clínico, específicamente el tratamiento de las imágenes diagnósticas.

El uso de la informática en aplicaciones clínicas es una constante hoy en día, especialmente en el campo del diagnóstico por imagen. La utilización de las placas digitales se ha ido imponiendo gracias a los avances tecnológicos, ya que suponen una mejor calidad de las mismas y la posibilidad de transmitirlas a distintos puntos de manera Inmediata.

El Colegio Americano de Radiología (ACR) y la Asociación Nacional de Fabricantes Eléctricos (NEMA) iniciaron un proyecto cuyos fines eran la elaboración de un estándar para la transferencia de imágenes y la información asociada a ellas que, tras varios intentos dio origen al formato DICOM 3.0.
Este se ha desarrollado para encontrar las necesidades que fabricantes y usuarios tienen con el equipamiento de la toma radiológica para la interconexión de dispositivos sobre redes convencionales.

2. DICOM (IMAGEN DIGITAL Y COMUNICACIÓN EN MEDICINA)

Son una serie de normas propuestas y administradas por la Asociación Nacional de Fabricantes Eléctricos (NEMA) [1], su principal propósito es garantizar la igualdad de condiciones desde el momento de la adquisición de un estudio imagenológico hasta el momento de ser desplegado en pantalla o impreso en papel radiográfico, después de un posible procesamiento gráfico [2].

La importancia que tienen las intensidades de grises es tal vez un factor determinante ya que estas deben ser las mismas sin importar el medio de visualización de la imagen, permitiendo que cualquier especialista observe lo mismo sin importar la naturaleza del medio de diagnóstico.

2.1 Estructura de archivo

Se define un lenguaje basado en un modelo propio del mundo real, es decir, todos los datos físicos o descriptivos como por ejemplo el nombre del paciente, el tipo de estudio, el dispositivo médico, los parámetros de la adquisición, tomadigital, etc., que son vistos por DICOM como elementos con sus respectivos atributos y propiedades [3]. De esta forma se establece una jerarquía entre los datos que permite realizar una clasificación según el contenido de la información por grupos, facilitando la identificación, el acceso a las variables y los parámetros de interés dentro de un mismo paquete [4].

El cuerpo del archivo se forma por una secuencia de “Conjuntos de datos” que a su vez están constituidos por “Elementos de datos” (ver Fig. 1), estos últimos son valores codificados de los atributos del objeto, identificados y clasificados por un “Tag”.

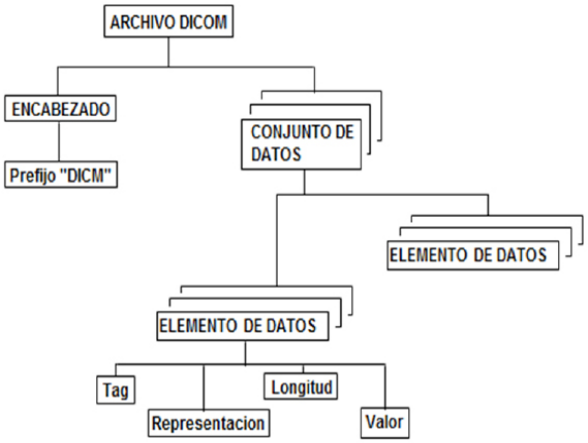

Fig. 1. Estructura de un archivo DICOM. [2]

Se utiliza la siguiente notación para referir a una etiqueta: (gggg,eeee), donde el primer valor hexadecimal de 2 bytes es el número de grupo y el segundo es el número del elemento. Por ejemplo (0010,0030) corresponde a la fecha de nacimiento del paciente.

También está compuesto por otros tres valores:

- El valor de representación (VR): indica el tipo de dato que se tiene almacenado.
- Longitud: especifica el tamaño ocupado por el "dato".
- Valor o el dato almacenado.

Existe una gran variedad de componentes y no siempre estarán definidos en su totalidad dentro de un archivo, así mismo habrá algunos que no aporten información relevante para ciertas necesidades. Por esto es importante saber que como mínimo el archivo debe contener los ítems mencionados en la tabla 1 para la adecuada lectura de la imagen.

La manera como están escritos los ítems mencionados en la tabla 1 se denominan Sintaxis de Transferencia, que generalmente es igual para todos los componentes de un archivo.

Tabla 1. Elementos de Datos necesarios para la lectura adecuada de una imagen diagnostica [2].

TAG	Descripción	Tipo
(0028,0002)	Samples per Pixel	Int
(0028,0008)	Number of Frames	Int
(0028,0010)	Rows	Int
(0028,0011)	Columns	Int
(0028,0100)	Bits Allocated	Int
(0028,0101)	Bits Stored	Int
(0028,0102)	Hight Bit	Int
(0028,0103)	Pixel Representation	Int
(0028,1050)	Windows Center	Int
(0028,1051)	Windows Width	Int
(0028,1052)	Rescale Intercept	Int
(0028,1053)	Rescale Slope	Int
(7FE0,0010)	Pixel data	Byte [] o Uint16 []

La manera como están escritos los ítems mencionados anteriormente (tabla 1) se denominan Sintaxis de Transferencia, que generalmente es igual para todos los componentes de un archivo.

La sintaxis de transferencia determina:

- Ordenamiento Big o Little Endian.
- Valor de representación (VR explícito o Implícito).
- Tipo de compresión de la imagen (Mapa de Bits, JPEG o diferentes tipos de compresión).

Los datos del píxel se pueden enviar en un formato nativo o en uno encapsulado definido fuera del estándar. Si están enviados en un formato nativo, las muestras del píxel se codifican como el encadenamiento directo de los bits de cada muestra del píxel. Si los bits están almacenados en un formato encapsulado, las muestras del píxel se cifran según el proceso de encriptación definido por uno de las sintaxis de transferencia [2]. Por lo general un archivo DICOM es reconocible por su extensión *.dcm, sin embargo, esto no es una exigencia, por lo que la forma de diferenciarlo es por medio del header o cabecera que consta de:

- 128 bytes de preámbulo que pueden estar en blanco o contener información sobre la aplicación principal con la que debe ser ejecutado [2].
- 4 bytes de prefijo “DICM”.

Como ejemplo, véase Fig. 2, un archivo DICOM donde la imagen tiene dimensiones de 109 x 91 x 2 pixeles con una resolución de datos de 1 byte por pixel, es decir, el tamaño total de la imagen es 19838 bytes.

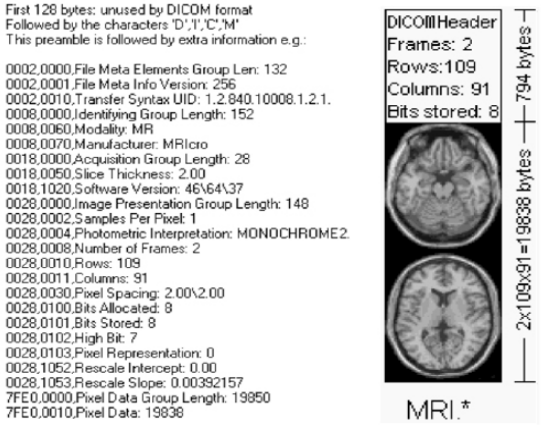

Fig. 2. Elementos de una estudio DICOM [5].

3. COMPONENTES BÁSICOS DE UN SISTEMA DE TRANSMISIÓN DE IMÁGENES MÉDICAS

La teleradiologia es la transmisión electrónica de imágenes radiológicas de pacientes [6], tales como tomografía computarizada, ultrasonido, resonancia magnética y rayos x entre otras, de un lugar a otro para propósitos de diagnóstico y revisión.

Un sistema básico consiste en 3 componentes fundamentales [7]:

- Estación de envío.
- Red de transporte.
- Estación de recepción / visualización.

En la Fig. 3 se muestra el flujo de trabajo típico en un hospital, donde un medico a través de una estación de visualización pregunta al servidor por un determinado examen, este verifica si lo contiene según los que tenga almacenados (previamente enviados por las estaciones) y se lo devuelve si efectivamente existe. Finalmente el medico recibe el estudio y puede emitir un concepto.

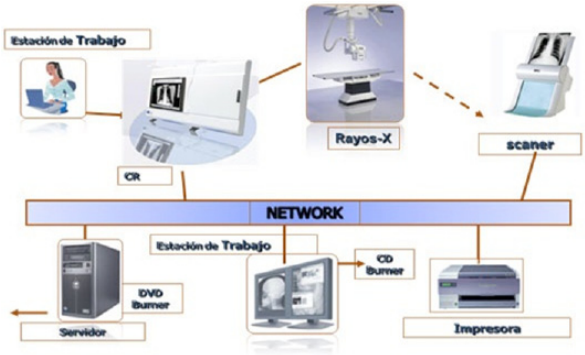

Fig. 3. Esquema general de un sistema de Teleradiologia [8].

3.1 Estación de envío

Consiste básicamente de:

- Digitalizador
- Dispositivo de red (Modem, tarjeta de red)

El digitalizador como su nombre lo dice convierte la imagen a un formato binario (1/0), donde los datos son enviados al dispositivo de red, este, se encarga de convertirlos en pulsos eléctricos y posteriormente enviarlos por la red de transporte.

Las tres especificaciones más importantes para estas estaciones son: resolución, compresión y velocidad de transmisión [6].

3.1.1 Resolución

Es la capacidad de un sistema de imágenes para diferenciar objetos [6]. Cuando una estación de envío digitaliza una película de rayos x, ésta queda distribuida en una matriz de dos dimensiones de pequeños elementos llamados píxeles. La información contenida en cada uno de ellos es asignada a un número que representa la cantidad (densidad) de información que contiene.

Este número es llamado número escala de gris.

3.1.2 Compresión

Es una técnica de software utilizada para disminuir tiempo de transmisión mediante el descarte de cierta cantidad de información, es comúnmente expresada como una relación (x:y), por ejemplo 10:1 significa que por cada píxel de información contenido en la matriz original 10 han sido omitidos después de la transmisión.

3.1.3 Velocidad de transmisión

Una estación de envío debería comprometer elevada resolución con baja compresión y con una velocidad de transmisión alta (cientos de Mbits/s [9]), sin embargo, esto no es tan sencillo de lograr debido a que la optimización de alguno de estos parámetros afecta a los demás (al incrementar la resolución se aumenta el tiempo de envío). La selección de la velocidad de transmisión se realiza teniendo en cuenta un punto de equilibrio de 700 Kbps que no afecta en mayor medida la resolución y la compresión. Teniendo en cuenta que los requisitos mínimos para la transmisión son [10]:

- Subida 750 Kbps (ideal 2000 Kbps o superior)
- Descarga 600 Kbps (ideal 2000 Kbps o superior)

3.2 Estación de recepción – visualización

Es la encargada de recibir y organizar la toma radiológica, que luego será desplegada en los monitores de diagnóstico. Los componentes más importantes de una estación de recepción-visualización son:

- Dispositivo de red.
- Computador.
- Software de procesamiento de imagen.
- Monitores de diagnóstico.

3.3 Técnicas de adquisición de imagenes diagnósticas

Permiten explorar el cuerpo humano, o partes de él, para la investigación en la ciencia médica o con propósitos clínicos (procedimientos médicos que buscan revelar, diagnosticar o examinar enfermedades) o para el guiado de la terapia, sea ésta quirúrgica o radioterapia.

En un sentido más estricto, son un conjunto de técnicas que producen imágenes del interior del cuerpo de forma no invasiva, con el fin aportar información sobre su estructura y funcionamiento, y ayudar así a detectar posibles anomalías en el mismo [11].

Mientras se desarrolla la tecnología y los conocimientos sobre la patología de enfermedades, se utilizan diversas combinaciones de tomas diagnósticas para promover un enfoque múltiple e integrado. En algunos casos, las tecnologías de adquisición, que ya se han utilizado por más de una década, se están cambiando y se están utilizando de una manera nueva. Estos cambios pueden facilitar el proceso de evaluación, haciéndolo menos invasivo, o incluso pueden crear nuevos métodos de diagnosticar las enfermedades [12].

3.3.1 Compresión

Son aquellas que aprovechan la propiedad de ionización de la materia, extrayendo los electrones de sus estados ligados al átomo.

Algunas ampliamente utilizadas son:

- Rayos X.
- Tomografía computarizada.
- Rayos Gamma.
- Tomografía por Emisión de Positrones.

3.3.2 Técnicas de diagnóstico basadas en la utilización de radiaciones no ionizantes

Son aquellas que utilizan ondas o partículas que no son capaces de arrancar electrones de los átomos, produciendo a lo sumo excitaciones electrónicas. Entre las técnicas que emplean este tipo de radiación cabe

destacar las siguientes:
- Resonancia magnética.
- Ultrasonido.

4. IMPLEMENTACIÓN DE PROTOCOLOS DE COMUNICACIÓN SEGUROS EN DICOM

La parte 15 de la norma concerniente al estándar provee un método normalizado para asegurar la comunicación y verificación de firmas digitales, sin embargo no especifica políticas de seguridad [13]. Solo establece mecanismos que pueden utilizarse para aplicarlas en relación con el intercambio de objetos entre entidades de aplicación.

Por ejemplo, una política de seguridad puede indicar un cierto nivel de control de acceso. Esta norma no tiene en cuenta los manejos de control de acceso, pero sí proporciona los medios tecnológicos a las entidades de aplicación interesadas.

Una vez conocidos los conceptos básicos del estándar con sus respectivos elementos y especificaciones, así como las recomendaciones para asegurar la comunicación entre entidades, se realiza la exploración dos de los protocolos ampliamente utilizados en comunicaciones seguras: IPSec y SSL.

Dentro del contexto del modelo de interconexión OSI-ISO, y a manera de información, en la tabla 2 se muestra la ubicación de algunos de los protocolos de criptografía más utilizados y reconocidos como estándares por la IETF. Las dos primeras capas están sujetas a los estándares de interoperabilidad de seguridad de LAN (SILS) [14].

Tabla 2. Capas y protocolos de criptografía [14].

Capa	*Nombre*	*Protocolos*
7	Aplicación	X.400, MSP, PEM, S/MIME, PGP, X.500, DNSSEC, Administración de certificados y llaves
6	Presentación	
5	Sesión	SSL
4	Transporte	TLSP
3	Red	NLSP, ESP, AH
2	Enlace de datos	SILS
1	Física	Enlace síncrono

Los protocolos IPSec y SSL son objeto de estudio en este trabajo, cada uno tiene ventajas y desventajas ya sea en términos de seguridad, integridad, confidencialidad y velocidad de transmisión.

4.1 Comunicación DICOM con soporte de seguridad basado en Ipsec (protocolo de seguridad de internet)

Es un conjunto de reglas cuya función es asegurar las comunicaciones sobre IP autenticando y/o cifrando cada paquete en un flujo de datos, incluye también mecanismos para el establecimiento de claves de cifrado [15].

Su objetivo principal es proporcionar protección a los paquetes IP, está basado en un modelo de seguridad de extremo a extremo, lo que significa que los únicos hosts que tienen que conocer la protección de IPSec son el que envía y el que recibe. Cada equipo controla la seguridad por sí mismo en su extremo, bajo la hipótesis de que el medio por el que se establece la comunicación no es seguro [16].

Sus principales características son:

- Autenticación mutua de los equipos antes del intercambio de datos.
- Establecimiento de una asociación de seguridad entre equipos, es decir, se puede implementar para proteger las comunicaciones entre usuarios remotos y redes, entre redes e, incluso, entre equipos cliente dentro de una red de área local (LAN).
- Cifrado de los datos intercambiados mediante estándar de cifrado de datos (DES), triple DES (3DES) o DES de 40 bits.
- Utiliza formatos de paquete IP estándar en la autenticación o el cifrado, por lo tanto, los dispositivos de red intermedios, como enrutadores, no pueden distinguir los paquetes de IPSec de los paquetes IP normales [16].

El flujo de comunicación DICOM con sopor-

te IPSec se muestra en la Fig. 4. Tanto el SCU (usuario de servicios de clase) como el SCP (proveedor de servicios de clase) obtienen los certificados por la misma entidad emisora (CA). Luego viene el intercambio de llaves (IKE), en este punto el protocolo de gestión de claves y la asociación de seguridad de internet (ISAKMP) se ejecutan en el SCP y el SCU para negociar los parámetros IKE e intercambiar certificados. Ahora el SCU y el SCP establecen la asociación con el estándar y la asociación IPSec. Ambos sitios inician la negociación de parámetros IPSec y crean una llave de sesión, utilizada para la comunicación de los datos. Finalmente se transmiten los datos por el canal seguro.

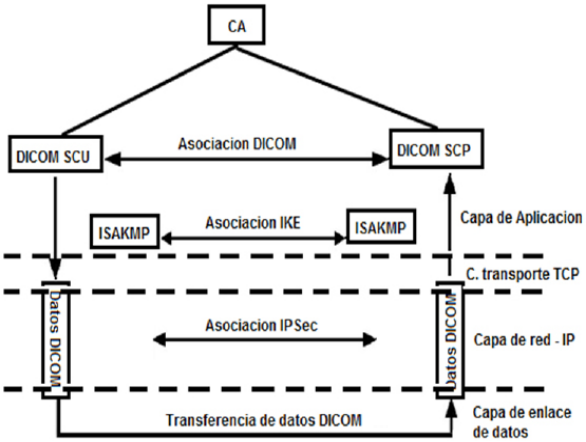

Fig. 4. Comunicación DICOM basada en IPSec [13].

4.2 Comunicación DICOM con soporte de seguridad basado en SSL (capa de conexión segura)

Diseñado originalmente por Netscape Development Corporation con el objetivo de establecer una conexión segura (con criptografía) entre cliente y servidor, proveer privacidad y confidencialidad en la comunicación de dos aplicaciones.

Arquitectónicamente está compuesto por dos capas:

En la capa inferior, se encuentra el protocolo SSL de registro, trabaja sobre algún protocolo de transporte (TCP o UDP), y se utiliza para encapsulamiento, cifrado, autenticación, servicios de secuencia y compresión [14].

En la capa superior se encuentran 4 protocolos:

SSL de inicio de comunicación entre dos entidades o handshake encargado de negociar mecanismos de codificación, autenticación, secuencia y compresión y establece los parámetros clave entre cliente y servidor.

Cambio de especificaciones de cifrado, invoca cambios síncronos de mecanismos de seguridad y parámetros clave entre cliente y servidor.

Protocolo de datos de aplicación para transportar los mensajes de aplicación entre los pares de cliente y servidor.

Protocolo de Alerta, que comunica mensajes de cierre y error de conexión.

La forma de establecer una conexión segura está basada en los siguientes servicios:

1. La conexión es privada, en el handshake inicial se define la llave secreta, y el algoritmo simétrico (DES, RC4, por ejemplo).
2. El cliente puede autenticarse utilizando algún algoritmo asimétrico o de llave pública (RSA, DSS, etc.). Esto es opcional, depende de si los certificados de cliente están disponibles.
3. El servidor se autentica utilizando certificados X.509.
4. La conexión es confiable. Se garantiza la integridad del mensaje utilizando funciones hash seguras MAC (SHA, MD5, etc.).
5. Se garantiza una secuencia estricta de mensajes, confía en TCP.
6. La compresión es opcional.

El flujo de datos de una comunicación DICOM con soporte SSL se muestra en la Fig. 5. Las entidades SCU (usuario de servicios

de clase) y SCP (proveedor de servicios de clase) obtienen los certificados de la misma entidad (CA). Después se establece la asociación correspondiente al estándar donde se ejecuta el handshake. Ahora el SCU transforma los datos en un formato SSL y lo envía al SCP por un canal seguro. Finalmente el SCP realiza el proceso inverso y obtiene los datos DICOM originales.

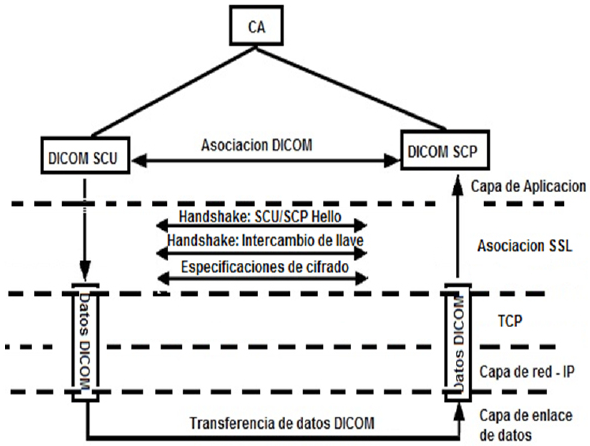

Fig. 5. SSL para establecer una comunicación DICOM segura entre cliente y servidor [13].

A continuación se realiza una comparación técnica de los dos protocolos escogidos teniendo en cuenta aspectos de autenticación, modo de conexión, orden de cifrado y tamaño de cabecera.

4.2.1 Algoritmo de autenticación

IPSec soporta el uso de firma digital y el uso de algoritmo de llave secreta, mientras que SSL solo soporta el uso de firma digital.

4.2.2 Método de autenticación

IPSec solo soporta un método de autenticación, mientras que SSL soporta varios tipos de autenticación, tal como se observa en las tablas 3 y 4 respectivamente.

Tabla 3. Método de autenticación IPSec [16].

Método de autenticación	Algoritmo de autenticación
Autenticación mutua	PSK
	RSA/DSA firma digital
	RSA llave publica
	KINK

Tabla 4. Método de autenticación SSL [16].

Método de autenticación	Algoritmo de autenticación
Autenticación del servidor	RSA (challenge/response)
	DSA firma digital
Autenticación del cliente	RSA/DSA firma digital
Anónimo	Ninguno

4.2.3 MAC

MAC (Authentication MessageCode - Código de autenticación de mensajes) es utilizado para legitimización de los mismos, después que se haya establecido la conexión. Tanto IPSec como SSL requiere la implementación de HMAC-SHA-1 y HMAC-MD5. HMAC es una función Hash que requiere una llave secreta para producir un resumen del mensaje. La fortaleza del algoritmo de Hash se basa en la longitud de la salida tal como se observa en la tabla 5.

Tabla 5. Tipos de algoritmos HMAC [16].

Protocolo	Algoritmo MAC	Longitud Hash
IPSec	HMAC-SHA-1-96	12 bytes
	HMAC-MD5-96	12 bytes
SSL	HMAC-SHA-1	20 bytes
	HMAC-MD5	16 bytes

4.2.4 Modo de conexión

IPSec tiene dos modos de conexión:

1. *Modo túnel.* Establecido entre Gateway a

Gateway, Gateway a Host y Host a Host. Se establece un túnel entre el extremo y requiere la adición de una nueva cabecera IP al paquete original [16].

2. *Modo transporte.* Es una conexión Host a Host. Los datos entre las dos entidades son encriptados [16].

La ventaja del modo túnel es la eliminación del "overhead" causado por cada canal. Pero la desventaja es que la conexión puede quedar expuesta si la llave ha sido comprometida.

SSL tiene una situación diferente. SSL es una conexión según el tipo de sesión. Cada sesión es independiente, pero el rendimiento puede caer si aumenta el número de sesiones.

4.2.5 Orden de las operaciones de cifrado

Como muestra la Fig. 6, IPSec primero cifra los datos y después crea la MAC. Si un dato modificado fuera insertado en medio de la transacción, IPSec puede verificar la MAC antes de realizar el descifrado.

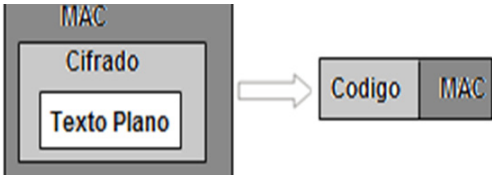

Fig. 6. Orden de cifrado IPSec [16].

SSL es diferente como se muestra en la Fig. 7, primero crea la MAC para los datos planos y luego cifra los datos. En el extremo, SSL debe descifrar primero y luego verificar la MAC, esto puede producir gasto innecesario de CPU descifrando paquetes modificados.

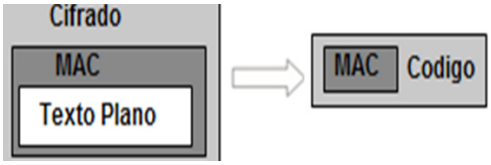

Fig..7. Orden de cifrado SSL [16].

4.2.6 Tamaño de cabecera

Una desventaja de IPSec es el tamaño extra agregado al paquete original, SSL requiere menos "overhead" que IPSec. La tabla 6 muestra el tamaño en bytes según el tipo de conexión.

Tabla 6. Tamaño cabecera [16].

Protocolo	Modo	Tamaño byte
IPSec modo túnel	ESP	32
	ESP y AH	44
IPSec modo transporte	ESP	36
	ESP y AH	48
SSL	HMAC-MD5	21
	HMAC-SHA-1	25

4.2.7 Resultados experimentales

Tomando como referencia los resultados obtenidos por Jianguo Zhang, FenchaiYu, y JianyongSun [6] se evaluó la velocidad de transmisión para comunicación de imágenes utilizando DICOM con tres diferentes parámetros:

1. El protocolo TCP/IP versión 4 para dos sistemas operativos diferentes
2. Configuración de los protocolos de seguridad IPSEC y SSL/TLS
3. Tamaño de las PDU

Cabe destacar que solo interesa conocer el comportamiento de mejor desempeño en velocidad para diferentes algoritmos y protocolos sin entrar en detalles específicos.

Velocidad de transmisión sin implementar seguridad

A continuación se grafican los datos obtenidos en [6] para comparar la velocidad de transmisión para diferentes modalidades (CT: tomografía computada, MR: resonancia magnética, CR: radiografía computada, US: ultrasonido) tanto en Linux como en Windows con diferentes valores de PDU. En la Fig. 8 se muestra el escenario utilizado en [6] para obtener los resultados:

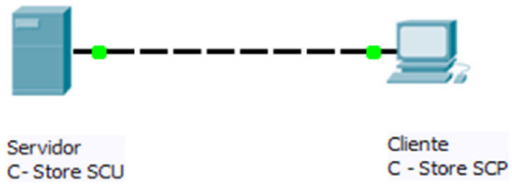

Fig. 8. Escenario de pruebas.

C-store SCU: Computador Dell Dimension, CPU Intel P4: 2.8Ghz, RAM: 512 MB, NCI: 100Mb/s, Disco duro: 80GB-IDE.

C-store SCP: Computador Dell Dimension, CPU Intel P4: 2.8Ghz, RAM: 512 MB, NCI: 100Mb/s, Disco duro: 80GB-IDE.

Sistemas operativos: Red Hat Enterprise Linux V3.0 y Microsoft Windows XP Professional Edition.

Así mismo el conjunto de imágenes utilizado en [6] es (no se utiliza ningún tipo de compresión):

- CT: Una serie con 100 imágenes DICOM (512x512x2b), tamaño total de 53.016Mb.
- MRI: Una serie con 200 imágenes DICOM (256x256x2b), tamaño total de 35.219 Mb.
- CR: 10 imágenes DICOM (2048x2495x2b), tamaño total de 89.150Mb.
- US: un archivo DICOM multiframe, tamaño total de 135.322Mb.

La tabla 7 muestra los resultados de velocidad (Kb / s) obtenidos para diferentes modalidades de imagen sin implementar ningún tipo de seguridad con sistema operativo Windows, claramente se observa que la modalidad que representa mayor velocidad es la de CR (radiografía Computada) y la de menor es la de MR (resonancia Magnética).

Tabla 7. Velocidades de transmisión (Kb/s) de imágenes usando DICOM con sistemas operativo Windows [6].

SISTEMA OPERATIVO WINDOWS			
Modalidad	(PDU 4096)	(PDU 16384)	(PDU 65536)
CT	2543	1219	1192
MR	843	530	558
CR	9203	8995	8878
US	7783	7151	6651

Una representación gráfica de la tabla 7 es mostrada en la Fig. 9, como se puede ver, el valor de PDU que muestra mejor desempeño es de 4096, frente al de 65536 que es de menor rendimiento.

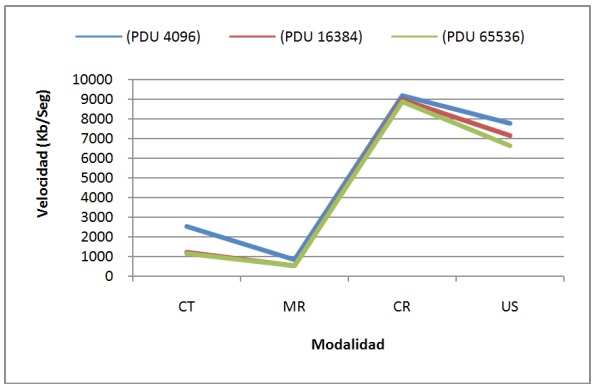

Fig. 9. Comparación de velocidad de transmisión para diferentes PDU en Windows.

Una representación gráfica de la tabla 8 muestra los resultados de velocidad (Kb / s) obtenidos sin implementar ningún tipo de seguridad con sistema operativo Linux. Se puede apreciar un mejor desempeño comparado con Windows, esto debido a que la utilización de recursos en Linux es mucho menor. En este caso la modalidad con mayor velocidad es la de US (ultrasonido) con CR (radiografía computada) y la de menor es la de MR (resonancia Magnética), también se observa un incremento en la velocidad para US, sin embargo se mantiene el mismo comportamiento para las demás modalidades. La explicación a esto se debe

a que el conjunto de imágenes que componen un estudio de ultrasonido representan mayor cantidad pero individualmente requieren menos memoria.

Tabla 8. Velocidades de transmisión (Kb/s) de imágenes usando DICOM con sistemas operativo Linux [6].

SISTEMA OPERATIVO LINUX			
Modalidad	(PDU 4096)	(PDU 16384)	(PDU 65536)
CT	2715	2732	2762
MR	1046	1063	1066
CR	9926	9893	9888
US	10100	10131	10186

El comportamiento de la velocidad de los datos de la tabla 8, es mostrado en la Fig. 10, se puede apreciar claramente que no hay una diferencia significativa entre modalidades para diferentes valores de PDU.

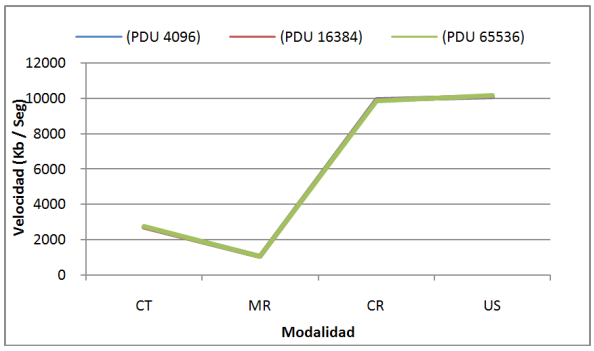

Fig. 10. Comparación de velocidad de transmisión para diferentes PDU en Linux.

Velocidad de transmisión con SSL e Ipsec

Seguidamente se compara IPSec y SSL con DES-CBC y AES 256 para diferentes tamaños de PDU.

La tabla 9 muestra los resultados de velocidad cuando se implementa IPSec y SSL con algoritmo DES-CBC con sistema operativo Linux, bajo estas condiciones ya se observa una disminución en la velocidad de transmisión con respecto a las condiciones de no implementación de seguridad.

Tabla 9. Velocidades de transmisión (Kb/s) de imágenes usando DICOM con algoritmos de encriptación DES-CBC con sistema operativo Linux [6].

ALGORITMO DE ENCRIPTACION DES-CBC		
Modalidad	(PDU 4096) SSL	(PDU 4096) IPSec
CT	2442	2670
MR	952	995
CR	9362	9696
US	9286	9923

La Fig. 11 es una gráfica de los datos de la tabla 9, como se puede ver IPSec muestra mayor velocidad, esto se debe a que requiere menos tiempo en el establecimiento de sesión como si lo requiere SSL [16] aunque la diferencia no es muy significativa.

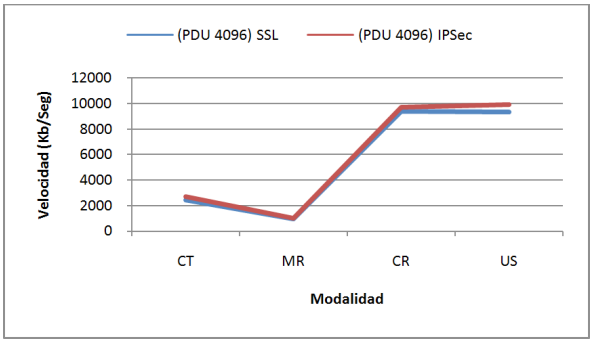

Fig. 11. Comparación de velocidad de transmisión para diferentes PDU para IPSec y SSL con DES-CBC. Autoría propia.

Ahora se verifica el comportamiento de velocidad de transmisión cuando se ha implementado un algoritmo más robusto como AES256, la tabla 10 muestra los resultados para esta situación y la figura 12 muestra la comparación de velocidad entre las diferentes modalidades. Se puede ver que la velocidad se mantiene casi en los mismo valores que en el caso anterior DES-CBC tanto para IPSec como para SSL. Aunque hay estudios [3] y [17] que demuestran que AES es más rápido que DES, por lo tanto es importante explorar con detenimiento las condiciones con las que se obtuvieron los resultados.

Tabla 10. Velocidades de transmisión (Kb/s) de imágenes usando DICOM con algoritmos de encriptación AES256 [6].

ALGORITMO DE ENCRIPTACION AES256		
Modalidad	(PDU 4096) SSL	(PDU 4096) IPSec
CT	2446	2678
MR	946	1032
CR	9360	9513
US	9593	9772

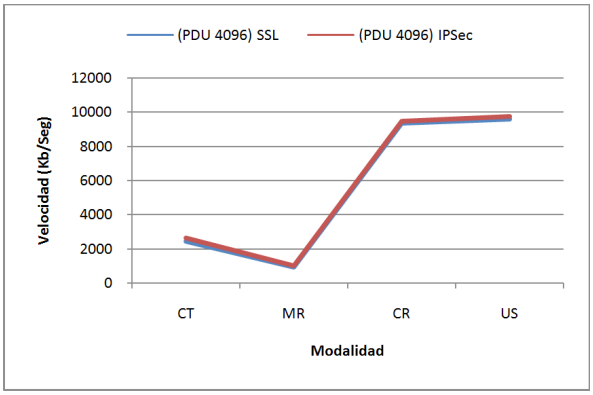

Fig. 12. Comparación de velocidad de transmisión para diferentes PDU para IPSec y SSL con AES256. Autoría propia.

5. CONCLUSIONES

Evidentemente el uso de protocolos de seguridad en la transmisión de imágenes diagnosticas medicas refleja una disminución en la velocidad de transmisión de cerca del 8% para el peor de los casos (ultrasonido utilizando SSL con DES) y por lo tanto un aumento en el tiempo de llegada de estas imágenes a su destino, esto se debe a que la inclusión de algoritmos seguros implica mayor tiempo de ejecución estableciendo sesiones e intercambiando claves entre entidades.

En términos de velocidad de transmisión no hay una diferencia muy significativa que permita descartar uno de otro (SSL o IPSec), aunque si se determinó que el sistema operativo con mejor desempeño es Linux frente a Windows.

En términos de facilidad de implementación, IPSec toma significativa ventaja frente a SSL, debido a que no requiere modificación a nivel de aplicación como si lo puede requerir SSL, muchas aplicaciones de diagnóstico médico no soportan SSL, por lo que es necesario buscar aplicaciones complementarias para implementarlo.

En la actualidad los servidores PACS de mayor uso como DCM4CHEE [18], OSIRIX [19], CLEARCANVAS [20] de naturaleza libre o código abierto soportan protocolos SSL, sin embargo debido la arquitectura del protocolo IPSec, éste se hace adaptable a cualquier servidor PACS, independientemente de la naturaleza comercial o no de estos servidores.

En términos de autenticación, SSL demuestra más robustez ya que permite varios tipos de autenticación tanto para cliente como para servidor. IPSec solo soporta un método de autenticación [16].
Teniendo en cuenta velocidad de transmisión y autenticación, el elegido seria SSL ya que aunque es un poco más lento que IPSec no representa una diferencia significativa mientras que si representa mayores prestaciones en términos de autenticación, sin embargo en escenarios reales que no soporten SSL la única opción es implementar IPSec.

Referencias Bibliográficas

[1] Página oficial de DICOM, [en línea]. Consultado el 2 de Marzo de 2010, disponible en:http://medical.nema.org.

[2] Descripción del estándar DICOM para un acceso confiable a la información de las imágenes médicas. Scientia et Technica Año XVI, No 45, Agosto de

2010. Universidad Tecnológica de Pereira.

[3] O.Pianykh, Digital Imaging and Communications in Medicine. A Practical Introduction and survival Guide, [en línea]. Consultado en marzo 3 de 2010, disponible en: http://ieeexplore.ieee.org/search/freesrchabstract.jsp?tp=&arnumber=1462682&queryText%3Ddicom%26openedRefinements%3D*%26searchField%3DSearch+All.

[4] Digital Imaging and Communications in Medicine. Part 4. Services class specifications, [en línea]. Consultado en Marzo 26 de 2010, disponible en:ftp://medical.nema.org/medical/dicom/2009/09_04pu.pdf.

[5] Digital Imaging and Communications in Medicine. Part 1. Introduction and Overview, [en línea]. Consultado en Marzo 26 de 2010, disponible en:ftp://medical.nema.org/medica/dicom/2009/09_04pu.pdf.

[6] DICOM Image Secure Communications with Internet Protocols Ipv6 and Ipv4. IEEE Transactions of information technology in biomedicine. Vol 11.No. 1. , Minnesota, USA January 2007.

[7] SajeeshKumar, Elizabeth A. Krupinski: Teleradiology, Springer, 2008, 284 paginas.pdf consultado el 19 de Marzo de 2010.

[8] Medingenium S.A. de C.V. 2010. Teleradiologia, [en línea]. Consultado en Marzo 19 de 2010, disponible en:http://www.medingenium.com.mx/telemedicina.html.

[9] An experimental teleradiology transmission system using a high-speed ATM backbone network. Department of Radiology, Nagoya University School of Medicine, Japan. Kato K, Shimamoto K, Ishigaki T, Niimi R, IshiguchiT, Mimura T, Yamauchi K, Ikeda M, Iwata A. J Telemed Telecare. 2000.

[10] Requisitos técnicos para la transmisión de imágenes Diagnósticas en Colombia, [en línea]. Consultado en mayo 10 de 2010, disponible en:http://www.teleradiologia.com.co/Teleradiologia_de_Colombia/Requisitos_tecnicos.html

[11] Diagnóstico por imagen. Estudio de prospectiva. Maribel Narvaez, Eva Merello. FundacionOpti. Federación de empresas de tecnología sanitaria, [en línea]. Consultado en Abril 23 de 2010, disponible en:http://www.fenin.es/pdf/diagnostico_imagen.

[12] Información esencial sobre imágenes diagnósticas, [en línea]. Consultado en Abril 23 de 2010, disponible en:http://www.angiomaalliance.org/pages.aspx?content=208&id=198.

[13] Digital Imaging and Communications in Medicine.Part15. Security and system management profiles, [en línea]. Consultado en Marzo 26 de 2010, disponible en:ftp://medical.nema.org/medical/dicom/2009/09_15pu.pdf

[14] María Concepción Mendoza Díaz, "Protocolos de seguridad e instrumentación de IPSec en escenarios experimentales de Internet 2 en México", Departamento de Ciencias de la Computación. Centro de investigación científica y de educación Superior de Ensenada. Ensenada, Baja California, México. Enero de 2002,[en línea]. Consultado en Marzo 19 de 2010, disponible en:http://seguridad.cudi.edu.mx/publications/tesis_comedi.pdf.

[15] Universidad Politécnica de Madrid, [en línea]. Consultado en Marzo 21 de 2010, disponible en:http://laurel.datsi.fi.upm.es/proyectos/teldatsi/teldatsi/protocolos_de_comunicaciones/protocolo_ipsec.

[16] A Technical Comparison OfIPSec and SSL. Abdel Nasir. Takamichi Saito. Tokyo University of Technology, [en línea]. Consultado en Marzo 21 de 2010, disponible en: http://www.net.in.tum.de/fileadmin/bibtex/publications/papers/niedermayer-mmb06.pdf

[17] Algoritmo de Encriptación AES, [en línea]. Consultado en Mayo 9 de 2010, disponible en: http://www.

icommcorp.com/downloads/Comparison%20AES%20vs%203DES.pdf
[18] Open Source Clinical Image and Object Management, [en línea]. Consultado en Mayo 10 de 2010, disponible en:http://www.dcm4che.org: en línea.
[19] Osirix Image Software, [en línea]. Consultado en Mayo 8 de 2010, disponible en: http://www.osirix-viewer.com en línea.
[20] Clear Canvas Software. Consultado en Abril 18 de 2010, disponible en: http://www.clearcanvas.ca en línea.
[21] A Web-based DICOM-Format Image Archive, Medical Image Compression and DICOM Viewer System for Teleradilogy Application, [en línea]. Consultado en Abril 18 de 2010, disponible en: http://ieeexplore.ieee.org/search/freesrchabstract. jsp?tp=&arnumber=5602817&queryText%3Ddicom%26openedRefinements%3D*%26searchField%3DSearch+Al .
[22] Dicom Works Teleradiology: Secure transmission of medical images over the Internet at low cost, [en línea]. Consultado en Abril 21 de 2010, disponible en: http://www.ncbi.nlm.nih.gov/pubmed/18003565
[23] Potential Impact of HITECH Security Regulations on Medical Imaging. 31st Annual International Conference of the IEEE EMBS. Minneapolis, Minnesota, USA, September 2-6, 2009.
[24] Medical Image Archiving, Processing, Analysis and Communication System for Teleradiology. TENCON 2010, [en línea]. Consultado en Marzo 26 de 2010, disponible en: http://ieeexplore.ieee.org/search/freesrchabstract.jsp?tp=&arnumber=4232675&queryText%3Ddicom%26openedRefinements%3D*%26searchField%3DSearch+All.
[25] Digital Imaging and Communications in Medicine. Part 8.Network communication support for message exchange, [en línea]. Consultado en Marzo 26 de 2010, disponible en:ftp://medical.nema.org/medical/dicom/2009/09_08pu.pdf.
[26] Técnicas de Imágenes diagnósticas. Sociedad Española de Reumatologia. pdf, [en línea]. Consultado en Abril 24 de 2010, disponible en: http://www.ser.es/D1F40A10-99F0-448C-857C02474FF3B814/FinalDownload/DownloadId-FCB1787622CEEE-858835584520B66F9E/D1F40A10-99F0-448C-857C-02474FF3B814/ArchivosDESCARGABLES/Dosieres_prensa/Imagen.pdf