SEGURIDAD EN REDES DE COMUNICACIÓNES ÓPTICAS

Taller N°9

Ronaldo Alexander Almachi Murillo, Dennys Francisco Salazar Domínguez
Escuela Politécnica Nacional
Quito, Ecuador
ronaldo.almachi@epn.edu.ec, dennys.salazar@epn.edu.ec

Resumen: En el siguiente documento se presenta una investigación con respecto a la seguridad en redes de comunicaciones ópticas, dicha investigación consiste en la resolución a una serie de preguntas como lo son descripción de los principales problemas de seguridad en redes ópticas, también se indica mecanismos para proveer servicios de seguridad y finalmente se realiza una breve descripción acerca de normativas y estándares con respecto a la seguridad en redes ópticas.

Palabras clave: Seguridad, redes, mecanismos, amenazas, sistemas ópticos

I. INTRODUCCIÓN

La seguridad de red es cualquier actividad diseñada para proteger el acceso, el uso y la integridad de la red y los datos corporativos.[1]

- Incluye tecnologías de hardware y software.
- Está orientada a diversas amenazas.
- Evita que ingresen o se propaguen por la red.
- La seguridad de red eficaz administra el acceso a la red.

La seguridad de red combina varias capas de defensa en el perímetro y la red. Cada capa de seguridad de red implementa políticas y controles. Los usuarios autorizados tienen acceso a los recursos de red, mientras que se bloquea a los usuarios maliciosos para evitar que ataquen vulnerabilidades y amenacen la seguridad.[1]

La digitalización ha transformado al mundo. Ha cambiado nuestra manera de vivir, trabajar, aprender y entretenernos. Todas las organizaciones que quieren prestar los servicios que exigen los clientes y los empleados deben proteger su red. La seguridad de red también ayuda a proteger la información confidencial de los ataques. En última instancia, protege su reputación.[1]

II. PREGUNTAS

A. ***Describa los principales problemas, inconvenientes y amenazas de seguridad en redes ópticas.***

Describa los problemas de seguridad en las distintas porciones de la red (e.g., acceso, metro, etc.)

Las redes ópticas son vulnerables a varios tipos de brechas de seguridad o ataques, generalmente destinados a interrumpir el servicio u obtener acceso no autorizado a los datos transportados, es decir, escuchas clandestinas. Dependiendo del objetivo del ataque, las brechas de seguridad pueden inducir pérdidas financieras a los clientes o causar interrupciones del servicio en toda la red, lo que posiblemente lleve a enormes pérdidas de datos e ingresos. Por lo tanto, el conocimiento de las vulnerabilidades de seguridad y los métodos de ataque es un requisito previo para diseñar soluciones de seguridad de redes ópticas efectivas.

Caída al aire en redes ópticas

Aunque las fibras ópticas son inmunes a la interferencia electromagnética y no irradian señales transportadas al medio ambiente, la exposición de las redes ópticas a las escuchas entraña una amenaza de seguridad considerable. Las escuchas clandestinas en general tienen como objetivo obtener acceso no autorizado a los datos para recopilar o analizar el tráfico.

Las escuchas ocurren en todas las capas de la red, desde la aplicación hasta la capa física, y se revelan nuevas instancias casi a diario. Según el método de

realización, los ataques de escucha clandestina se pueden clasificar en:

- Ataques con acceso directo al canal óptico sin cifrar
- Ataques basados en violar la clave de cifrado en sistemas ópticos cifrados

Escuchas clandestinas a través del acceso al canal (ECA)

Un método común para realizar ataques de escucha clandestina es acceder directamente al canal óptico a través de la derivación de fibra, es decir, quitar el revestimiento de fibra y doblar la fibra para hacer que la señal se filtre fuera del núcleo y en el fotodetector, capturando la información.

Los dispositivos de roscado que se pueden sujetar a la fibra y hacer que las micro curvas emitan señales y las entreguen a las manos del fisgón son fácilmente accesibles en el mercado. Además, los dispositivos de escucha existentes causan pérdidas por debajo de 1 dB y pueden pasar desapercibidos por los sistemas de administración de red (NMS) de uso común. Para detectar tales intrusiones, NMS debe mejorarse con alarmas de detección de intrusiones activadas por cambios de pérdida de inserción en las conexiones de fibra. Obviamente, tales detecciones requieren un sistema de monitoreo activo que se ejecute en la red.

Otra forma posible de acceder al canal es a través de puertos de monitorización, que normalmente están presentes en diferentes componentes de la red, como amplificadores, conmutadores selectivos de longitud de onda (WSS) o (des) multiplexores. La señal óptica es reflejada por un divisor óptico para permitir la conexión de dispositivos de monitoreo sin interrupción del tráfico. Al obtener acceso en el sitio, un atacante podría usar estos puertos para escuchar el tráfico transmitido.

Escuchas a escondidas a través del acceso por clave (EKA)

Para proteger los datos transportados de escuchas, se utilizan métodos de encriptación, implementados en transpondedores ópticos. La mayoría de los proveedores comercializan estas tarjetas de cifrado. Un ejemplo de solución de Alcatel Lucent se basa en el cifrado de los paquetes de datos mediante claves de cifrado que se transfieren a través del NMS aislado de la carga útil de datos. Normalmente, las claves de cifrado las gestiona el usuario final. Sin embargo, el software de gestión de claves está instalado en el lado del usuario, lo que puede servir como otro punto de ataque que llegue al sistema NMS del operador.

Métodos de degradación del servicio

El objetivo de los ataques de degradación del servicio en la capa óptica es degradar la calidad del servicio o provocar la denegación del servicio, normalmente mediante la inserción de señales dañinas en la red.

Ataques de interferencia de alta potencia (HPJ)

La interferencia de alta potencia se realiza insertando una señal óptica de potencia excesiva (por ejemplo, 5 - 10 dB por encima de otras señales legítimas) en una longitud de onda legítima utilizada en la red.

En las redes compuestas por multiplexores ópticos de adición y caída (OADM) fijos sin ninguna funcionalidad de bloqueo de longitud de onda (por ejemplo, atenuadores ópticos variables), las señales de alta potencia pueden dañar las señales de usuario que se propagan conjuntamente dentro de sus fibras ópticas, amplificadores y conmutadores comunes. En los conmutadores ópticos, las señales de interferencia pueden afectar a las señales legítimas en la misma longitud de onda (indicadas como Usuario 1) aumentando la diafonía dentro de la banda. Señales que atraviesan el común los enlaces físicos con la señal de interferencia pueden sufrir efectos fuera de banda en fibras ópticas y amplificadores.

En las fibras, las señales de interferencia dan lugar a diafonía fuera de banda al filtrarse a los canales vecinos y/o aumentar los efectos no lineales (Usuario 2). En amplificadores de fibra dopados con erbio (el tipo más comúnmente utilizado de amplificadores), una señal de interferencia fuera del rango de trabajo puede causar la denominada competencia de ganancia, en la que las señales legítimas más débiles (Usuarios 2 y 3) pierden ganancia debido a la señal de interferencia más fuerte, mientras que la señal de ataque obtiene adicionalmente amplificado.

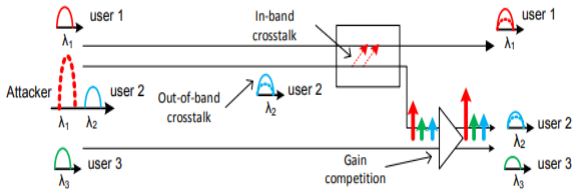

Fig. 1. Efectos de una señal de interferencia de alta potencia dentro de fibras ópticas, interruptores y amplificadores.

Ataques de longitud de onda alienígena (AWA)

Para permitir las actualizaciones de la red y la transmisión eficiente de conexiones de alta capacidad sobre la infraestructura existente, los operadores se ven obligados a implementar longitudes de onda extrañas en su red. La Figura 1 muestra una red de múltiples proveedores con y sin soporte de longitud de onda alienígena. Cuando no hay soporte de longitud de onda extraterrestre, cada la conexión es terminada y regenerada por un nodo en el borde del dominio (nodo B1 para la conexión verde).

Las longitudes de onda alienígenas, por otro lado, pueden atravesar múltiples dominios sin conversiones ópticas / electrónicas / ópticas (O / E / O) (conexión roja). Otro ejemplo del uso de longitudes de onda extraterrestres es actualizar los sistemas de línea heredados con transpondedores de nueva generación 100G. Estas soluciones se utilizan ampliamente en las implementaciones actuales.

La presencia de longitudes de onda alienígenas puede crear una vulnerabilidad significativa para la seguridad de la red dependiendo de la gestión de longitudes de onda alienígenas. Aproximadamente el 40% de las redes actuales siguen siendo redes punto a punto simples y fijas basadas en OADM, en las que el sistema de control y gestión no tiene información sobre el rendimiento de los canales ajenos. En consecuencia, la potencia y la frecuencia de la señal no se pueden controlar. Además, si los nodos de la red se basan en divisores y WSS en una configuración de transmisión y selección, las longitudes de onda extraterrestres se lanzan en la red sin filtrar.

En tales sistemas, las longitudes de onda alienígenas pueden explotarse para realizar varios métodos de ataques (por ejemplo, interferencia) y presentan un gran riesgo para los proveedores de red. En las redes más inteligentes, las longitudes de onda alienígenas son administradas por el NMS, es decir, un canal se configura como una longitud de onda amigable, permitiendo que el sistema de administración tenga información de los parámetros de la señal, pero aún sin control sobre sus valores. En las redes de nueva generación, se define una interfaz dedicada para albergar longitudes de onda alienígenas con la función de sintonizar sus niveles de potencia, pero aun así no tendrá control de la frecuencia del canal alienígena.

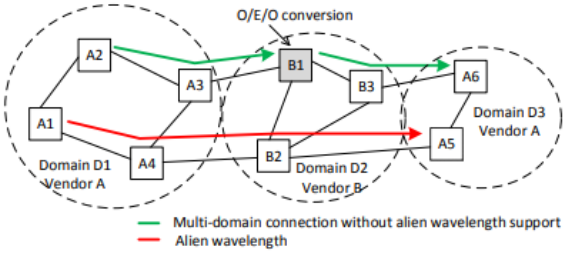

Fig. 2. Longitudes de onda extraterrestres no administradas en una red de múltiples proveedores que pueden actuar como señales de interferencia.

Ataques de inserción de señal en redes de velocidad de línea mixta (SIA-MLR)

Las redes de velocidad de línea mixta (MLR) representan una solución intermedia y rentable para la actualización gradual de la red de las rutas de luz heredadas de 10 Gbit/s a 40/100/200 Gbit/s al permitir la coexistencia de diferentes formatos de modulación sobre la infraestructura existente.

Una vulnerabilidad de seguridad clave de las redes MLR se debe a los efectos no lineales entre las señales 40/100/200G y los canales vecinos 10G heredados. Es decir, los canales 10G con modulación de amplitud en canales desactivados (OOK) deterioran en gran medida la calidad de los canales con modulación de fase de mayor velocidad de bits debido a la modulación de fase cruzada (XPM).

En el caso de canales multiplexados por polarización, la modulación por polarización cruzada (XPolM) afecta adicionalmente a la transmisión óptica, en redes gestionadas por dispersión de forma aún más dominante que XPM. Aunque es técnicamente posible tener canales de 10G y 40/100/200G en un espaciado de 50 GHz,

esto impone una penalización adicional de OSNR para los canales de 40/100/200G.

La gravedad de dicha penalización depende del formato de modulación, la potencia de lanzamiento del canal y las bandas de guarda. En la mayoría de las redes desplegadas no es posible cambiar el formato de modulación ni las potencias de lanzamiento, quedando solo la opción de utilizar bandas de guarda entre canales 40/100/200G y 10G. Un posible ataque de degradación del servicio en las redes MLR, podría infligirse insertando un canal OOK cerca de un canal 40/100/200G, sin permitir suficiente banda de guarda. Por lo tanto, la señal de ataque podría deteriorar significativamente el OSNR de las señales legítimas.

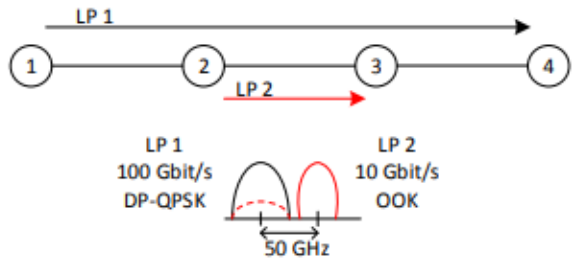

Fig. 3. Ataque de inserción de señal en una red de velocidad de varias líneas: la señal de 100 Gbit/s modulada en fase sufre un aumento de los efectos XPM de una señal de 10 Gbit/s modulada en amplitud.

Inserción de señal en ataques de puertos de monitoreo (SIM)

Los componentes totalmente ópticos están equipados con puertos de monitoreo externos, que dan lugar a ciertas vulnerabilidades de seguridad. Además de proporcionar un medio para posibles escuchas clandestinas, los puertos de monitoreo también podrían usarse para insertar señales en la red y dañar el tráfico en vivo.

B. Indique los mecanismos para proveer servicios de seguridad en redes de comunicaciones ópticas.

Indique aspectos consideraciones técnicas que deben ser cubiertas para que una red de comunicaciones ópticas se considere segura y/o resiliente.

La seguridad de la red óptica puede protegerse eficazmente mediante métodos basados en fibra, incluido el procesamiento de señales ópticas, distribución de claves ópticas, esteganografía y comunicación ópticas basada en el caos. [2]

Los dispositivos basados en fibra no irradian una firma electromagnética y son inmunes a la interferencia electromagnética, por lo que el adversario no puede escuchar a escondidas.[2]

Confidencialidad

La confidencialidad de los datos garantiza que los datos confidenciales no se divulguen a un usuario no autorizado en la red. En una red de fibra óptica, el intruso puede recibir diafonía residual de un canal adyacente o tocando físicamente la fibra óptica. El cifrado óptico y la codificación óptica pueden proteger eficazmente la confidencialidad de la red de capa física y satisfacer los requisitos de alta velocidad de las redes modernas. Como los dispositivos basados en fibra no generan radiación electromagnética, los procesos de codificación y encriptación óptica son inmunes a los ataques basados en la firma electromagnética de la señal. En esta sección, primero proporcionamos ejemplos de cifrado óptico y analizamos sus aplicaciones en la comunicación segura. A continuación, resumimos brevemente una técnica CDMA óptica. Por último, describimos los métodos de distribución de claves para el cifrado y la codificación.[2]

Cifrado óptico

El cifrado protege la transmisión de datos cifrando los datos originales en texto cifrado. Sin conocer la clave del proceso de cifrado, el intruso no puede recuperar los datos. El cifrado óptico ha sido ampliamente estudiado en la literatura. En comparación con los circuitos electrónicos, los dispositivos de transmisión y procesamiento óptico tienen menor latencia y mayor velocidad. Otra motivación para el cifrado óptico es que los dispositivos basados en fibra no generan una firma electromagnética. La señal en la fibra no irradia una señal electromagnética ni está bloqueada por interferencias electromagnéticas externas. Si bien, en comparación con el cifrado electrónico, el cifrado óptico tiene una funcionalidad limitada, sigue desempeñando un papel importante en áreas que requieren tanto una seguridad sólida como una velocidad de procesamiento rápida. Por ejemplo, el cifrado óptico podría ser especialmente importante en el ámbito del comercio de alta frecuencia.[2]

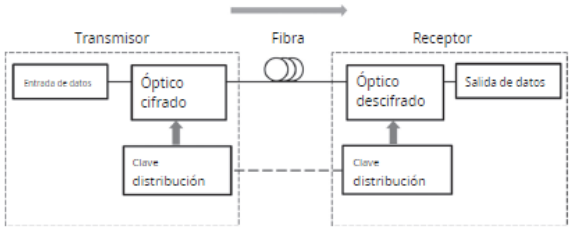

Fig. 4 Esquema de cifrado óptico

CDMA óptico

El CDMA óptico protege la confidencialidad de los datos mediante el uso de un patrón de código para representar los bits "0" y "1". Varios usuarios con códigos diferentes (ortogonales) pueden compartir el mismo canal para transmitir datos simultáneamente. El CDMA óptico se puede dividir en dos categorías: CDMA óptico coherente y CDMA óptico incoherente. Un sistema CDMA óptico coherente típico usa codificación de fase espectral, que da diferentes cambios de fase a los componentes espectrales coherentes en el transmisor. Para decodificar la señal, se utilizan desplazamientos de fase conjugados en el receptor. Un esquema de CDMA óptico incoherente típico se denomina ensanchamiento de tiempo de salto de longitud de onda (WHTS). WHTS utiliza pulsos incoherentes en diferentes longitudes de onda para representar una secuencia de código. Dentro de cada secuencia de código, cada pulso tiene un retardo diferente y ocupa un chip de tiempo diferente en cada bit. El receptor de una secuencia de código deseada compensa los retrasos de los diferentes pulsos para formar un pico de autocorrelación (ACP). La aplicación de la misma compensación de retardo a las otras secuencias de códigos no deseadas forma una función de correlación cruzada y, debido a la naturaleza ortogonal de los códigos, esto da como resultado una interferencia de acceso múltiple (MAI). Para mejorar la relación señal-ruido (SNR), se puede utilizar un umbral óptico para suprimir el MAI.[2]

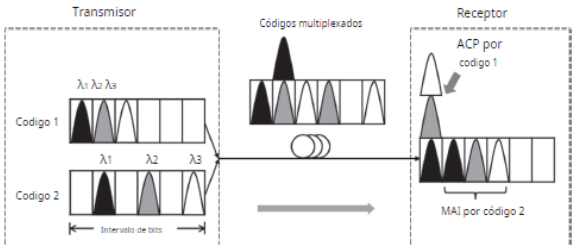

Fig. 5 Esquema CDMA óptico

Distribución de claves ópticas

Aunque el cifrado óptico y la codificación óptica pueden proteger eficazmente la confidencialidad de la capa física, la clave para el proceso de cifrado y descifrado debe distribuirse de forma segura entre los usuarios autorizados. La clave se puede transmitir a una velocidad menor que los datos cifrados, pero requiere un nivel de seguridad más alto. La distribución de claves cuánticas puede proteger eficazmente el proceso de cifrado al codificar la información clave sobre los estados cuánticos de un solo fotón.[2]

Privacidad y esteganografía óptica

La privacidad garantiza el control individual de qué información se puede recibir o recopilar y a quién se puede transmitir o divulgar la información. Aunque el cifrado de datos puede proteger los datos originales en un canal de señal para que no sean recibidos por el intruso, no puede proteger la existencia del canal para que no sea detectado. En algunos casos, el sistema ya está amenazado si el adversario conoce la existencia de un canal privado. El objetivo de la esteganografía óptica en una red de comunicación por fibra es ocultar señales en los canales públicos existentes para que el fisgón no pueda recibir las señales ni detectar la existencia del canal oculto.[2]

El canal oculto, que transporta las señales furtivas, está diseñado de tal manera que nadie, aparte del destinatario previsto, puede detectar la existencia de la señal en el dominio del tiempo o en el dominio espectral. Para enterrar el canal sigiloso en el ruido que ya existe en el sistema, la potencia de la señal sigilosa es típicamente 10 dB 20 dB más baja que la del canal público. La esteganografía óptica fue propuesta y demostrada experimentalmente por primera vez por Wu et al.[2]

El enfoque básico en la esteganografía óptica es estirar temporalmente un pulso óptico corto a través de la dispersión cromática. Sin utilizar la compensación de dispersión correcta en el receptor, la señal estirada queda enterrada en el ruido del sistema del canal público. En el dominio espectral, debido a que el ancho espectral del pulso óptico es del orden de varios nanómetros, que es mucho más amplio que el espectro del canal público, el espectro óptico del canal sigiloso se fusiona con el ruido de fondo del canal público.[2]

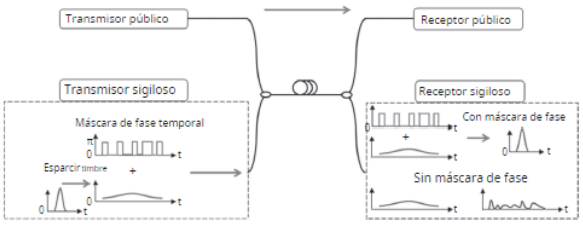

Fig. 6 Diagrama esquemático para la modulación de fase temporal en pulsos furtivos extendidos

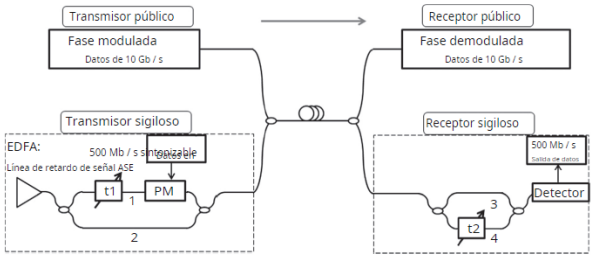

Fig. 7 Diagrama esquemático para esteganografía óptica basada en ruido de emisión espontánea amplificada

Disponibilidad

Jamming y anti-jamming

La "disponibilidad" es un aspecto de la seguridad que garantiza que no se niegue un servicio de red a los usuarios autorizados. Una posible amenaza para la disponibilidad de la red es bloquear un canal de señal con ruido fuerte. La esteganografía óptica basada en ruido ASE, que se analiza en la última sección, puede proteger eficazmente la disponibilidad cuando la señal es transportada por ASE, que cubre toda la banda de transmisión (conocida como la "banda C") para comunicaciones de fibra óptica. Esto aumenta la dificultad de realizar interferencias maliciosas, e incluso si el adversario pudiera interferir en toda la banda C, no quedaría ancho de banda para su propia comunicación de datos. Otra posible solución para garantizar la disponibilidad utiliza la conversión de banda de ondas. En este esquema, se utilizan múltiples bandas de ondas para la comunicación. Si la banda de ondas actual se atasca, el canal de datos se puede convertir hacia arriba o hacia abajo a un nuevo rango de banda de ondas. La conversión de banda de ondas se puede implementar con un litio de polos periódicos niobato (LiNbO3) material, lo que resulta en una penalización de baja potencia y BER.[2]

Comunicaciones ópticas basadas en el caos

Las comunicaciones basadas en el caos proporcionan un enfoque para transmitir datos confidenciales con un alto nivel de solidez. La señal caótica de banda ancha no solo mejora la robustez de la transmisión de datos a una interferencia de banda estrecha o interferencia maliciosa, sino que también se puede utilizar para bloquear la comunicación de los adversarios. A diferencia de la esteganografía óptica, que tiene como objetivo reducir la amplitud de la señal sigilosa lo más pequeña posible, la estrategia de las comunicaciones basadas en el caos es enmascarar los datos confidenciales con un caos mucho más fuerte. La generación del caos se basa en la señal de entrada, por lo que solo el receptor que tiene conocimiento de cómo se genera el caos puede reproducir el caos y cancelarlo para recuperar la señal.[2]

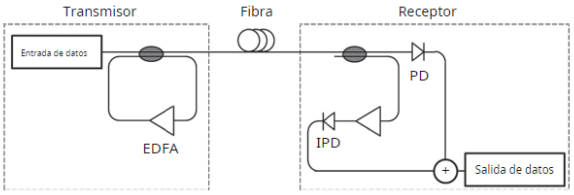

Fig. 8 Diagrama esquemático para la comunicación óptica del caos

C. <u>De existir, indique la normativa o estándares (e.g., de la ITU vigentes relacionadas con aspectos de seguridad en redes ópticas)</u>

Describa los estándares y describa los aspectos técnicos y procedimientos que considere más relevantes

Arquitectura de seguridad de la interconexión de sistemas abiertos para aplicaciones del CCITT

Recomendación X.800

La Recomendación X.200 del CCITT describe el modelo de referencia básico para la interconexión de sistemas abiertos (ISA). Dicha Recomendación establece un marco para coordinar el desarrollo de Recomendaciones existentes y futuras para la interconexión de sistemas.[3]

El objetivo de la ISA es permitir la interconexión de sistemas de computador heterogéneos de modo que puedan lograrse comunicaciones útiles entre procesos de aplicación. En distintos momentos, deben establecerse controles de seguridad para proteger la información intercambiada entre los procesos de aplicación. Estos controles deben hacer que el costo de obtener o modificar los datos de una manera indebida sea mayor que el valor potencial de esta acción, o hacer que el tiempo requerido para obtener los datos de una manera indebida sea tan largo que pierdan su valor.[3]

Descripción general de los servicios y mecanismos de seguridad. [3]

Visión de conjunto

En este punto se examinan los servicios de seguridad que se incluyen en la arquitectura de seguridad de ISA y los mecanismos que realizan estos servicios. Los servicios de seguridad descritos a continuación son servicios de seguridad básicos. En la práctica, se invocarán en las capas apropiadas y en combinaciones apropiadas, usualmente con servicios y mecanismos que no son de ISA, para satisfacer la política de seguridad y/o las exigencias de los usuarios. Pueden utilizarse mecanismos de seguridad particulares para realizar combinaciones de los servicios de seguridad básicos. En las realizaciones prácticas de los sistemas pueden utilizarse combinaciones particulares de los servicios de seguridad básica invocación directa.

Servicios de seguridad

Se considera que los siguientes servicios de seguridad pueden proporcionarse facultativamente en el marco del modelo de referencia de ISA. Los servicios de autenticación requieren información de autenticación que comprende información almacenada localmente y datos que se transfieren (credenciales) para facilitar la autenticación.

- *Autenticación*

  Estos servicios proporcionan la autenticación de una entidad par comunicante y de la fuente de datos, según se describe a continuación.

  Autenticación de entidad par

  Este servicio se utiliza en el establecimiento de la fase de transferencia de datos de una conexión, o a veces durante ésta, para confirmar la identidad de una o varias entidades conectadas a una o varias otras entidades. Este servicio da confianza, en el momento de utilización solamente, en que una entidad no está tratando de usurpar otra identidad o la reproducción no autorizada de una conexión anterior. Son posibles esquemas de autenticación de entidad par unilaterales y mutuos, con o sin comprobación en tiempo real, y pueden proporcionar diversos grados de protección.

  Autenticación del origen de los datos

  El servicio de autenticación del origen de los datos confirma la fuente de una unidad de datos. Este servicio no proporciona protección contra la duplicación o modificación de las unidades de datos.

- *Control de acceso*

  Este servicio proporciona protección contra el uso no autorizado de recursos accesibles mediante ISA. Estos recursos a los que se tiene acceso mediante protocolos de ISA, pueden ser o no de ISA. Este servicio de protección puede aplicarse a diversos tipos de acceso a un recurso (por ejemplo, el uso de un recurso de comunicaciones, la lectura, la escritura, o la supresión de un recurso de información; la ejecución de un recurso de procesamiento) o a todos los accesos a un recurso

- *Confidencialidad de los datos*

  Estos servicios proporcionan la protección de los datos contra la revelación no

autorizada, según se describe a continuación.

- Confidencialidad de los datos en modo con conexión
- Confidencialidad de los datos en modo sin conexión
- Confidencialidad de campos seleccionados
- Confidencialidad del flujo de tráfico

- *Integridad de los datos*

  Estos servicios contrarrestan las amenazas activas y pueden ser de una de las formas descritas a continuación.

  Integridad en modo con conexión con recuperación: Este servicio proporciona la integridad de todos los datos de usuario (N) en una conexión (N) y detecta cualquier modificación, inserción, supresión o reproducción de cualquier dato dentro de una secuencia completa de UDS (con tentativa de recuperación).

  Integridad en modo con conexión sin recuperación: Igual que el anterior, pero sin tentativa de recuperación.

  Integridad de campos seleccionados en modo con conexión: Este servicio proporciona la integridad de campos seleccionados en los datos de usuario (N) de una UDS (N) transferida por una conexión y adopta la forma de una indicación que permite saber si los campos seleccionados han sido modificados, insertados, suprimidos o reproducidos.

  Integridad en modo sin conexión: Este servicio proporciona la integridad de una sola UDS en modo sin conexión y puede adoptar la forma de una indicación que permite saber si una UDS recibida ha sido modificada. Además, puede proporcionarse una forma limitada de detección de reproducción.

  Integridad de campos seleccionados en modo sin conexión: Este servicio proporciona la integridad de campos seleccionados dentro de una sola UDS en modo sin conexión y adopta la forma de una indicación que permite saber si los campos seleccionados han sido modificados.

- *No repudio*

  Este servicio puede adoptar una de las formas siguientes o ambas.

  No repudio con prueba del origen: Se proporciona al destinatario de los datos la prueba del origen de los datos. Esto lo protegerá contra cualquier tentativa del expedidor de negar que ha enviado los datos o su contenido.

  No repudio con prueba de la entrega: Se proporciona al expedidor de los datos la prueba de la entrega de los datos. Esto lo protegerá contra cualquier tentativa ulterior del destinatario de negar que ha recibido los datos o su contenido.

Mecanismos de seguridad específicos

Los siguientes mecanismos pueden incorporarse en la capa (N) apropiada para proporcionar algunos de los servicios descritos en el punto anterior.

- *Cifrado*

  El cifrado puede proporcionar la confidencialidad de la información de datos o del flujo de tráfico y puede desempeñar una función en varios otros mecanismos de seguridad o complementarlos.

- *Mecanismos de firma digital*

  La característica esencial del mecanismo de firma es que la firma sólo puede producirse utilizando la información privada del firmante. De este modo, cuando se verifica la firma, puede probarse subsiguientemente a una tercera parte (por ejemplo, a un juez o árbitro), en cualquier momento, que sólo el

poseedor único de la información privada pudo haber producido la firma

- *Mecanismos de control de acceso*

  Estos mecanismos pueden utilizar la identidad autenticada de una entidad o información sobre la entidad (tal como la lista de miembros de un conjunto conocido de entidades) o capacidades de la entidad, para determinar y aplicar los derechos de acceso de la entidad. Si la entidad intenta utilizar un recurso no autorizado, o un recurso autorizado con un tipo impropio de acceso, la función de control de acceso rechazará la tentativa y puede informar además el incidente a los efectos de generar una alarma y/o anotarlo en el registro de auditoría de seguridad. La notificación al expedidor del rechazo de acceso para una transmisión de datos en modo sin conexión puede proporcionarse solamente como resultado de controles de accesos impuestos en el origen.

- *Mecanismos de integridad de los datos*

  La integridad de los datos tiene dos aspectos: la integridad de una sola unidad de datos o de un solo campo, y la integridad de un tren de unidades de datos o de campos de unidad de datos. En general, se utilizan diferentes mecanismos para proporcionar estos dos tipos de servicios de integridad, aunque no es práctica la provisión del segundo sin el primero.

- *Mecanismo de intercambio de autentificación*

  Los mecanismos pueden incorporarse en la capa (N) para proporcionar autenticación de la entidad par. Si el mecanismo no logra autenticar la entidad, el resultado será el rechazo o la terminación de la conexión y puede causar también una anotación en el registro de auditoría de seguridad y/o un informe a un centro de gestión de seguridad.

- *Mecanismo de relleno de tráfico*

  Pueden utilizarse mecanismos de relleno de tráfico para proporcionar diversos niveles de protección contra análisis del tráfico. Este mecanismo puede ser eficaz solamente si el relleno de tráfico está protegido por un servicio de confidencialidad.

- *Mecanismo de control de encaminamiento*

  La política de seguridad puede prohibir que los datos que transportan ciertas etiquetas de seguridad pasen a través de ciertas subredes, relevadores o enlaces. Asimismo, el iniciador de una conexión (o el expedidor de una unidad de datos en modo sin conexión) puede especificar prohibiciones de encaminamiento en las que se indica que se eviten determinadas subredes, enlaces o relevadores.

- *Mecanismo de notarización*

  Pueden garantizarse las propiedades sobre los datos comunicados entre dos o más entidades, tales como su integridad, origen, fecha y destino, mediante la provisión de un mecanismo de notarización. La seguridad es proporcionada por una tercera parte que actúa como notario, en el que las entidades comunicantes tienen confianza y que mantiene la información necesaria para proporcionar la garantía requerida de una manera verificable. Cada instancia de comunicación puede utilizar la firma digital, el cifrado y los mecanismos de integridad, según sea apropiado, para el servicio que es proporcionado por el notario. Cuando se invoca este mecanismo de notarización, los datos se comunican entre las entidades comunicantes por las instancias de comunicación protegidas y el notario.

Mecanismos de seguridad pervasivos

En este punto se describen varios mecanismos que no son específicos a un servicio particular. Algunos mecanismos de seguridad pervasivos pueden considerarse como aspectos de gestión de seguridad.

- *Funcionalidad de confianza*

La funcionalidad de confianza puede utilizarse para ampliar el campo de aplicación o para establecer la eficacia de otros mecanismos de seguridad. Toda funcionalidad que proporciona directamente mecanismos de seguridad o que permite el acceso a estos mecanismos deberá ser digna de confianza.

- *Etiquetas de seguridad*

  Los recursos que comprenden elementos de datos pueden tener asociadas etiquetas de seguridad, por ejemplo, para indicar un nivel de sensibilidad. A menudo es necesario transportar la etiqueta de seguridad apropiada con datos en tránsito. Una etiqueta de seguridad puede ser un dato suplementario asociado a los datos transferidos o puede estar implícita; por ejemplo, puede ser la consecuencia de la utilización de una clave específica para cifrar los datos o puede resultar del contexto de los datos, como la fuente o la ruta. Las etiquetas de seguridad explícitas deben ser claramente identificables, para poder verificarlas de manera apropiada. Además, deben estar vinculadas de una manera segura a los datos con los cuales están asociadas.

- *Detección de eventos*

  La detección de eventos relativos a la seguridad comprende la detección de violaciones aparentes de seguridad y puede incluir también la detección de eventos «normales» tales como el acceso logrado (o «log on»). Los eventos relativos a la seguridad pueden ser detectados por entidades, dentro de la ISA, que comprenden mecanismos de seguridad.

- *Registro de auditoría de seguridad*

  Los registros de auditoría de seguridad proporcionan un mecanismo de seguridad valioso dado que hacen posible detectar e investigar potencialmente las violaciones de seguridad permitiendo una auditoría de seguridad posterior. Una auditoría de seguridad es un estudio independiente y un examen de las anotaciones y de las actividades del sistema para probar la idoneidad de los controles, asegurar la coherencia con la política establecida y con los procedimientos de explotación, ayudar a evaluar los daños y recomendar modificaciones de los controles, de la política y de los procedimientos. Una auditoría de seguridad necesita la anotación de informaciones relativas a la seguridad en un registro de auditoría de seguridad, así como el análisis y la producción de informes a partir de las anotaciones que figuran en un registro de auditoría de seguridad.

- *Recuperación de seguridad*

  La recuperación de seguridad trata las peticiones provenientes de mecanismos tales como las funciones de tratamiento y de gestión de los eventos y realiza acciones de recuperación como resultado de la aplicación de un conjunto de reglas.

III. CONCLUSIONES

1. La seguridad para las redes ópticas es un tema muy importante y no solo es a nivel de software, interferencias, intrusos, sino también a nivel físico pues la fibra, antenas, equipos, etc., están involucrados es por ello que el estudio tanto a nivel computacional como en el mundo real es necesario para prevenir accidentes como robo de información, caídas de los enlaces, daños, que pueden implicar la integridad de los usuarios y asuntos económicos importantes y que pueden ser de alta gravedad ya que las telecomunicaciones conllevaatrás de ella grandes sumas de dinero como inversión y que se busca obtener posteriormente.
2. El cifrado dentro de las telecomunicaciones y hablando de redes ópticas no puede faltar y consisten en pasar de un lenguaje a otro con nivel de complejidad y mecanismos de seguridad

para asegurar los datos de los usuarios dentro de la red.

3. La fibra óptica como medio de transmisión es bastante seguro ya que se puede identificar con precisión el segmento de fibra que esta siendo vulnerado, sin embargo, como cualquier otro sistema de comunicaciones las vulneraciones se dan en los equipos del usuario o bases de datos con muy poca seguridad, a pesar de que en la fibra óptica se transmiten señales de luz las vulneraciones son un tanto diferentes y de la misma manera algunos métodos para contrarrestarlas.
4. La arquitectura de seguridad para una red de datos se puede aplicar no solo en una red óptica sino en una convencional, pero es importante recordar que la mayoría de enlaces de muy largas distancias que cubren continentes son de fibra óptica, por lo que los estándares están muy bien adaptados para redes ópticas.

IV. REFERENCIAS

[1] "¿Qué es la seguridad de red?", *Cisco*. https://www.cisco.com/c/es_mx/products/security/what-is-network-security.html (consultado ago. 10, 2021).

[2] B. Wu, B. Shastri, y P. Prucnal, "Secure Communication in Fiber-Optic Networks", en *Emerging Trends in ICT Security*, 2013, pp. 173–183. doi: 10.1016/B978-0-12-411474-6.00011-6.

[3] "X.800 : Arquitectura de seguridad de la interconexión de sistemas abiertos para aplicaciones del CCITT". https://www.itu.int/rec/T-REC-X.800-199103-I/es (consultado ago. 13, 2021).