ESCUELA POLITECNICA NACIONAL

FACULTAD DE ELECTRICA Y ELECTRONICA

SISTEMAS CELULARES

INTEGRANTES:

Cristian Gallo

Alejandra Silva

CURSO: GR1

FECHA: 2021-07-16

TALLER Nº9

Seguridad en redes de comunicaciones ópticas.

- **Describir los principales problemas, inconvenientes y amenazas, de seguridad en redes ópticas. Describir los problemas de seguridad en las distintas porciones de la red (acceso, metro, etc.)**

  Existe el riesgo de que alguien pueda conectarse a una conexión de fibra óptica. Por lo tanto, se debe proteger la fibra de la misma manera que aseguraría los medios de cobre. En concreto, se debe:

  - Colocar los tendidos de fibra de preferencia en conductos para evitar daños al cable y proporcionar una capa de protección contra los que deseen acceder al cable.
  - Utilizar encriptación para datos confidenciales. El uso de la encriptación agrega una capa adicional de seguridad que protege los datos en caso de que un atacante obtenga acceso a una transmisión de fibra [1].

  Aunque una red de fibra óptica tiene la reputación de ser inmune a los ataques de espionaje, existen ciertos tipos de ataques que son susceptibles el cable de fibra óptica como es la extracción de la señal por curvatura o empalmes, lo que le da acceso a un atacante a paquetes que atraviesan la conexión. Mientras que las escuchas en las conexiones de fibra son más difíciles que las conexiones de cobre, los atacantes con sofisticados conjuntos de habilidades y equipos pueden ser capaces de hacerlo. Además, las cantidades significativas de datos transportados sobre una conexión de fibra de alto ancho de banda presentan un objetivo atractivo para un atacante.

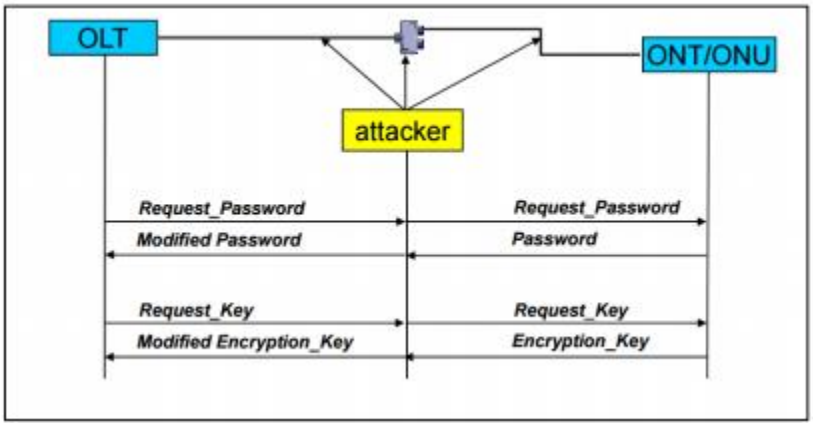
  Existen otras amenazas que pueden complicar la situación, como ataques de intervenir directamente al cable de fibra que forma parte de la red GPON, este caso se considera físicamente no realista puesto que el atacante debería realizar en lugares públicos y probablemente perturbaría toda la red GPON en la que pretende intervenir. La comunicación GPON es vulnerable a graves problemas de seguridad, estas amenazas de seguridad podrían ser tratadas con mecanismo de seguridad implementados en la capa física o en las capas superiores.

  OLT falsificado Actualmente no existen mecanismos de identificación y autenticación para la OLT, es por ello que el ONT / ONU no tiene medios para detectar el falso OLT. Desde la OLT se puede autenticar las unidades ONU/ONT por medio de un número serial, pero no hay forma de poder

autenticar la OLT lo que convierte en una amenaza, ya que si un atacante tiene acceso a la infraestructura de la red puede añadir un OLT falso, y así poder tener acceso a todo el tráfico que está cursando la red GPON.

Los ataques de (MITM) (Man In The Middle- Hombre en el Medio) ¬ Ataques pasivos: Contraseña y claves enviadas como texto claro. El atacante puede interceptar el tráfico de datos y la información sensible (sin cifrar) como contraseñas de autenticación y claves de cifrado, que se utilizarán posteriormente para, por ejemplo, interceptación ilegal. Se pude interceptar el tráfico, añadiendo un ONU/ONT falso a la red y así poder tener acceso a claves de autenticación o de cifrado ya que estas viajan en texto plano. También se puede interceptar el tráfico con el método de extracción de la señal de fibra óptica [1].

Ataque activo: Los mensajes sensibles de PLOAM no están autenticados, por ejemplo: contraseña, clave de encriptación. El atacante puede modificar información sensible (sin cifrar): contraseñas de autenticación y claves de cifrado para causar por ejemplo una denegación de servicio



La ONT/ONU puede transferir datos bidireccionalmente para iniciar el proceso de autenticación. Los datos son transmitidos por OLT en intervalos de tiempo, donde cada ONU tiene ranuras de tiempo propias que pueden utilizarse para la transmisión de datos. La propiedad más importante es que los datos no se cifran de ninguna manera. El atacante es capaz de leer las tramas en la dirección descendente, solo necesita acceso físico a la fibra o a un divisor. El divisor se encuentra a menudo en un lugar del edificio o en un lugar similar accesible al público. Si consideramos la dirección ascendente, los datos son transferidos por unicast [1].

Tipos de Ataques:

ATAQUES DE CONTRASEÑAS: Los principales métodos que se emplean para este tipo de ataques son fuerza bruta y ataque mediante diccionario. Estos ataques buscan conseguir nuestra contraseña para suplantarnos.

- **Ataques por fuerza bruta**: Los ataques por fuerza bruta se basan en la prueba de diferentes combinaciones secuenciales para finalmente descubrir nuestra credencial de acceso. Este tipo de ataques se basa en el tiempo por lo que muchos bots pasado un tiempo desisten y cambian de objetivo.
- **Ataques mediante diccionario**: los ataques basados en el uso de diccionario realizan una consulta a la base de datos de contraseñas comúnmente utilizadas u obtenidas mediante la falsificación de un acceso.

ATAQUES CON TÉCNICAS AVANZADAS DE INGENIERÍA SOCIAL: estos ataques van dirigidos directamente a nuestra información personal y a obtener el control de nuestros dispositivos. Los ataques suelen suplantar alguna web fraudulenta o un archivo con código malicioso para infectarnos con algún malware. Principalmente utilizan el engaño y la manipulación para conseguir directamente nuestros datos. Ataques mediante un mensaje suplantando la entidad original, existen varias técnicas en función del medio que se emplea: Phishing (mail, redes sociales o mensajería instantánea). Ataques mediante Baiting o gancho, se emplea un medio físico (por ejemplo, un pendrive) para utilizar nuestra curiosidad de que contiene e infectar nuestro equipo para conseguir nuestros datos personales.

ATAQUES A NUESTRAS CONEXIONES: Estos ataques buscan nuestras conexiones de acceso a Internet y nuestras redes wifi para monitorizar y conseguir nuestros datos. Las técnicas más empleadas por los atacantes son:

- Suplantación de redes libres o wifi con el fin de que pensemos que estamos empleando una red y sin embargo estamos conectados a una exactamente igual pero que va a conseguir todos nuestros datos. Esto puede ocurrir en lugares públicos que nos ofrecen servicios de acceso a Internet gratuitos.
- Suplantación de identidad personal, web o entidad para conseguir nuestros datos de acceso. A este tipo de ataque se le conoce genéricamente como Spoofing.

Ataques dirigidos a nuestras cookies: se aprovecha la comunicación un servidor http para conseguir nuestros datos.

Ataques de denegación de servicios: conocidos por DoS. Este tipo de ataque se basa en saturar un servicio mediante múltiples conexiones. Su objetivo es provocar la pérdida de un servicio para que nos sea posible su utilización. En este caso las recomendaciones son cuestión del administrador del servicio y no para los usuarios que intentamos acceder.

Ataques de inyección de código SQL: los sistemas de bases de datos SQL también son un objetivo frecuente para los ataques. En este caso se insertan fraudulentamente líneas de código SQL en el servicio, con el fin de obtener nuestros datos. Al igual que el caso anterior es cuestión del administrador del servicio y no de los usuarios que acceden. Sin embargo, en este caso sí que puede tener un efecto negativo en los usuarios.

Escaneo de puertos: su fin es comprobar que puertos tenemos abiertos en nuestro sistema para posteriormente analizar sus debilidades y proceder a realizar un segundo ataque mediante otra técnica, por ejemplo, denegación de servicio, contraseña o fuerza mayor.

ATAQUES POR MALWARE: estos ataques insertan en nuestro sistema un programa malicioso para conseguir nuestra información [2].

- **Indique los mecanismos para proveer servicios de seguridad en redes de comunicaciones ópticas. Indique aspectos o consideraciones técnicas que deben ser cubiertas para que una red de comunicaciones ópticas se considere segura y/o resilente.**

La categorización de los ataques se clasifica en seis áreas basado en el objetivo del atacante: Análisis de tráfico, Eavesdropping (escuchar secretamente), Retardos de datos, Negación de servicio, Degradación en la calidad de servicio (QoS), Spoofing (Suplantación de identidad).

La seguridad debe requerir dos requisitos básicos: el secreto y la autenticidad. El secreto se puede dividir en dos tipos: el secreto provisional, lo que significa la prevención de un usuario no autorizado de recibir los datos transmitidos, y el secreto de largo plazo, que es generalmente protegidos por criptografía compleja. La criptografía es parte de la seguridad, la cual es la protección del significado de los datos, incluso cuando un atacante tiene acceso al flujo de datos transmitidos. Se debe proporcionar una arquitectura segura en la red, en la cual tenga métodos y técnicas que pueden ser utilizados para prevenir o reducir el impacto de las amenazas [1].

La autorización y control de acceso en la seguridad en GPON proporciona protección contra la divulgación de información, robo de servicio, y la protección contra acceso no autorizado. Es necesario disponer de medidas de seguridad adicionales para el uso de GPON, como el proceso de limitar el acceso a los recursos del sistema y permitir que sólo los usuarios, programas, procesos u otros sistemas autorizados accedan al OLT, ya que es la parte más vital de la red.

La recomendación G.984.3 de GPON describe el uso de un mecanismo de seguridad de la información para asegurar que los usuarios puedan acceder únicamente a los datos destinados a ellos. Actualmente existen dos mecanismos de seguridad, ambos considerandos como opcionales.

- Autenticación de la ONU/ONT mediante contraseña (PLOAM)
- Cifrado en el tráfico descendente (desde CO al cliente), mediante AES (128 bit)

El tráfico ascendente no se considera en riesgo debido a que el tráfico ascendente presenta una arquitectura punto a punto, por lo que el tráfico enviado desde la ONT a la OLT no puede ser escuchado ni interceptado por otros ONTs. La arquitectura de protección de GPON se considera que mejora la fiabilidad de las redes de acceso. Sin embargo, la protección se considera como un mecanismo opcional porque su implementación depende de la realización de sistemas económicos. Hay dos tipos de conmutación de protección, conmutación automática y conmutación forzada. El primero es activado por la detección de fallos, tales como pérdida de señal, pérdida de trama, degradación de señal y así sucesivamente. El segundo es activado por eventos como el desvío de fibra, reemplazo de fibra, etc [1].

- **De existir indique la normativa o estándares (UIT) vigentes relacionados, con aspectos de seguridad en redes ópticas. Describa los estándares y describir los aspectos técnicos y procedimientos que considere más relevantes.**

Recomendaciones ITU

Series X: Data networks, open system communications and security
Las recomendaciones: X.800-X.849: Security

X.800: Security architecture for Open Systems Interconnection for CCITT applications

X.802: Information technology – Lower layers security model

X.803: Information technology – Open Systems Interconnection – Upper layers security model

X.805: Security architecture for systems providing end-to-end communications

X.810: Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview

X.811: Information technology – Open Systems Interconnection – Security frameworks for open systems: Authentication framewo

X.812: Information technology – Open Systems Interconnection – Security frameworks for open systems: Access control framewo

X.813: Information technology – Open Systems Interconnection – Security frameworks for open systems: Non-repudiation framew

X.814: Information technology – Open Systems Interconnection – Security frameworks for open systems: Confidentiality framewo

X.815: Information technology – Open Systems Interconnection – Security frameworks for open systems: Integrity framework

Fig. 1 Recomendaciones Series X.

Recommendation X.805 (10/03)
SERIE X: REDES DE DATOS Y COMUNICACIÓN ENTRE SISTEMAS ABIERTOS
Seguridad Arquitectura de seguridad para sistemas de comunicaciones extremo a extremo

Dimensiones de seguridad

Una dimensión de seguridad es un conjunto de medidas de seguridad que responden a un determinado aspecto de la seguridad de red. En esta Recomendación se identifican ocho conjuntos de medidas contra las principales amenazas. Las dimensiones de seguridad incluyen la red, las aplicaciones y la información de usuario de extremo. Además, se aplican a los proveedores de servicio y las empresas que ofrecen servicios de seguridad a sus clientes. Estas son las dimensiones de seguridad:

1) control de acceso;
2) autenticación;
3) no repudio;
4) confidencialidad de datos;
5) seguridad de la comunicación;
6) integridad de los datos;
7) disponibilidad;
8) privacidad.

Las dimensiones de seguridad definidas e implementadas correctamente soportan la política de seguridad definida para una determinada red y facilitan la aplicación de las normas de gestión de la seguridad [3].

Cuadro 1/X.805 – Las dimensiones de seguridad que corresponden a las amenazas

Dimensiones de seguridad	Amenazas contra la seguridad				
	Destrucción de información y otros recursos	Corrupción o modificación de información	Robo, supresión o pérdida de información y de otros recursos	Revelación de información	Interrupción de servicios
Control de acceso	Y	Y	Y	Y	
Autenticación			Y	Y	
No repudio	Y	Y	Y	Y	Y
Confidencialidad de datos			Y	Y	
Seguridad de la comunicación			Y	Y	
Integridad de los datos	Y	Y			
Disponibilidad	Y				Y
Privacidad				Y	

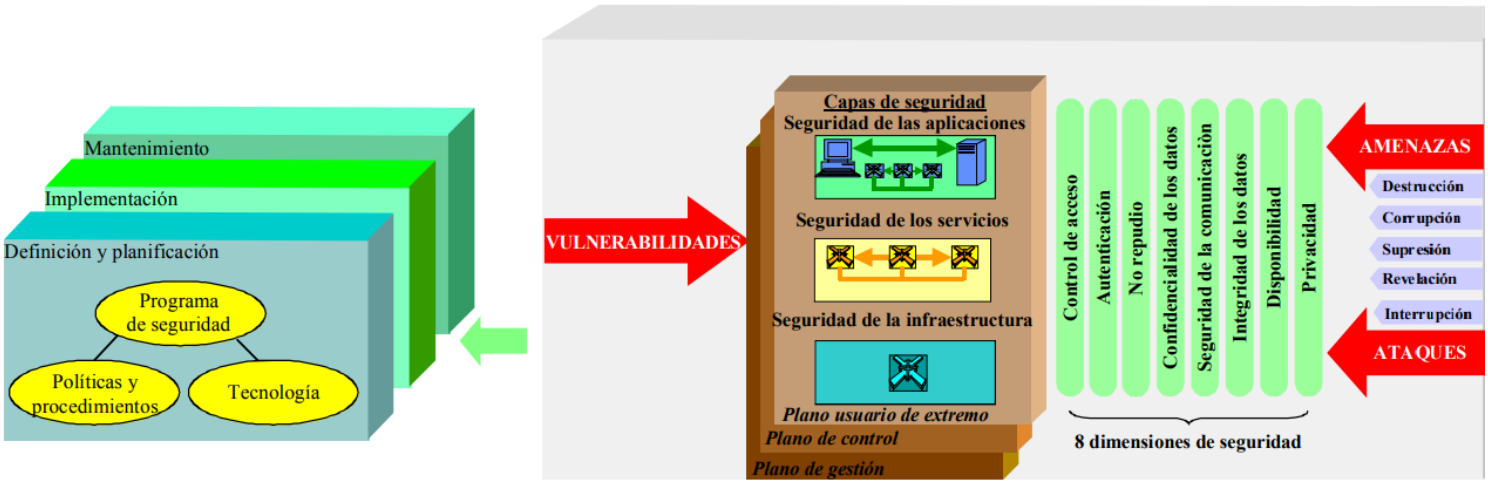


Fig. 2 Aplicación de la arquitectura de seguridad a los programas de seguridad.

Requisitos, Arquitecturas, Gestión de Seguridad [4]:

Tema	Subtema	Ejemplos de las Recomendaciones & publicaciones pertinentes
3. Requisitos de seguridad	3.2 Amenazas, riesgos y vulnerabilidades 3.3 Objetivos de seguridad 3.4 Razones para las normas de seguridad 3.6 Requisitos de seguridad personal y física	X.1205: Aspectos generales de la ciberseguridad E.408: Requisitos de seguridad para las redes de telecomunicaciones X.1051: Directrices basadas en la norma ISO/CEI 27002 para la gestión de la seguridad de la información para organizaciones de telecomunicaciones Tecnologías de planta externa para redes públicas Aplicación de ordenadores y microprocesadores a la construcción, instalación y protección de cables de comunicaciones
4. Arquitecturas de seguridad	4.1 Arquitectura de seguridad de sistemas abiertos 4.2 Servicios de seguridad 4.3 Arquitectura de seguridad para sistemas que proporcionan comunicaciones de extremo a extremo 4.3.2 Disponibilidad de la red y sus componentes 4.4 Directrices de implementación 4.5 Arquitecturas específicas de la aplicación	X.800: Arquitectura de seguridad de sistemas abiertos X.805: Arquitectura de seguridad para sistemas de comunicaciones extremo a extremo X.810: Marcos de seguridad: Visión general X.Sup3: Serie ITU-T X.800-X.849 – Suplemento sobre directrices para la implementación de la seguridad entre sistemas y redes X.1162: Arquitectura y operaciones de seguridad para redes entre pares X.1161: Marco para comunicaciones seguras entre pares X.1143: Arquitectura de seguridad para seguridad de mensajes en servicios móviles de la web
5. Gestión de seguridad	5.1 Gestión de seguridad de la información 5.2 Gestión de riesgos 5.3 Tratamiento de incidentes	X.1051: Directrices para la gestión de la seguridad de la información para organizaciones de telecomunicaciones X.1055: Guía para la gestión de riesgos y el perfil de riesgos E.409: Estructura para organizar los incidentes y solucionar los incidentes de seguridad

Directorio, Autenticación y gestión de identidad, Seguridad de Infraestructura [4]:

6. El directorio, autenticación y gestión de identidad	6.1 Protección de la información del directorio 6.1.4 Protección de privacidad 6.2 Mecanismos de seguridad de clave pública 6.2.3 Infraestructuras de clave pública 6.4 Gestión de identidad 6.5 Telebiométrica	X.500: Visión de conjunto de conceptos, modelos y servicios X.509: El directorio: Marcos para certificados de claves públicas y atributos X.1171: Amenazas y requisitos para la protección de información identificable personalmente en las aplicaciones que utilizan la identificación basada en las etiquetas Y.2720: Marco general para la gestión de identidades en las redes de la próxima generación X.1081: Marco para la especificación de los aspectos de la telebiometría relativos a protección y seguridad X.1089: Infraestructura de autenticación de telebiometría
7. Seguridad de la infraestructura de red	7.1 La red de gestión de las telecomunicaciones 7.2 Arquitectura de gestión de red 7.4 Seguridad de las actividades de supervisión y control 7.5 Seguridad de aplicaciones basadas en la red 7.6 Servicios comunes de gestión de la seguridad 7.6.4 Servicios de seguridad basados en CORBA	M.3010: Principios para una red de gestión de las telecomunicaciones X.790: Función de gestión de dificultades para aplicaciones del UIT-T X.711: Protocolo común de información de gestión X.736: Función señaladora de alarmas de seguridad X.740: Función de pista de auditoría de seguridad X.780: Directrices de la RGT para la definición de objetos gestionados CORBA

Planteamientos, Aplicaciones de Seguridad y Contrarrestar amenazas [4]:

8. Algunos planteamientos específicos de la seguridad de red	8.1 Seguridad de las redes de la próxima generación (NGN) 8.2 Seguridad de comunicaciones móviles 8.3 Seguridad para redes domésticas 8.4 Requisitos de seguridad para IPCablecom 8.6 Seguridad para redes de sensores ubicuos	Y.2001: Visión general de las redes de próxima generación Y.2701: Requisitos de seguridad de la versión 1 de la red de próxima generación X.1121: Marco general de tecnologías de seguridad para las comunicaciones móviles de datos de extremo a extremo X.1111: Marco de tecnologías de la seguridad para redes domésticas J.170: Especificación de la seguridad de IPCablecom
9. Aplicaciones de seguridad	9.1 Voz sobre IP (VoIP) y multimedios 9.2 IPTV 9.3 Facsímil seguro 9.4 Servicios de la web 9.5 Servicios basados en etiquetas	H.235: Marco de seguridad para sistemas multimedia de la serie H X.1191: Requisitos funcionales y arquitectura de los aspectos relativos a la seguridad de la TVIP T.36: Capacidades de seguridad para su utilización con terminales facsímil del grupo 3 X.1141: Lenguaje de etiquetas de aserción de seguridad (SAML 2.0)
10. Contrarrestar amenazas comunes de red	10.1 Contrarrestar el spam 10.2 Código malicioso, programas espía y software engañoso 10.3 Notificación y diseminación de actualizaciones del software	X.1231: Estrategias técnicas contra el correo basura X.1240: Tecnologías utilizadas contra el correo basura X.1244: Aspectos globales para contrarrestar el correo basura en las aplicaciones multimedios en las redes IP X.1207: Directrices para los proveedores de servicios de telecomunicaciones acerca del riesgo de programas espías y de software potencialmente no deseado X.1206: Marco independiente del proveedor para la notificación automática de información relacionada con la seguridad y para la difusión automática de actualizaciones

Bibliografía:

[1] J. A. Sigcho Poma, «Estudio de la seguridad en redes GPON.», abr. 2018, Accedido: ago. 11, 2021. [En línea]. Disponible en: https://dspace.unl.edu.ec//handle/123456789/20415

[2] «Conoce los Tipos de Ciberataques y las Mejores Prácticas -», *Ralco Networks*, nov. 23, 2020. https://www.ralco-networks.com/conoce-los-tipos-de-ciberataques-y-las-mejores-practicas/ (accedido ago. 11, 2021).

[3] «X.805 : Security architecture for systems providing end-to-end communications». https://www.itu.int/rec/T-REC-X.805-200310-I (accedido ago. 11, 2021).

[4] «T-HDB-SEC.04-2009-PDF-S.pdf». Accedido: ago. 11, 2021. [En línea]. Disponible en: https://www.itu.int/dms_pub/itu-t/opb/hdb/T-HDB-SEC.04-2009-PDF-S.pdf