124. LA SEGURIDAD EN REDES. TIPOS DE ATAQUES Y HERRAMIENTAS PARA SU PREVENCIÓN: CORTAFUEGOS, CONTROL DE ACCESOS E INTRUSIONES, TÉCNICAS CRIPTOGRÁFICAS, ETC. MEDIDAS ESPECÍFICAS PARA LAS COMUNICACIONES MÓVILES

Índice

1 INTRODUCCIÓN

Los conceptos que aparecen en este tema pueden aparecer en alguna pregunta del test del primer examen.

De cara al tercer ejercicio, es un tema relevante para representar las arquitecturas de red o física.

En color rojo se subrayan conceptos que han sido preguntados en exámenes oficiales.

El gobierno español, a instancia del Consejo de Seguridad Nacional aprobó el en abril de 2019 la Estrategia de Ciberseguridad Nacional. El documento presenta las características que definen el ciberespacio, se fijan las directrices generales para su uso seguro, se trazan los objetivos y se definen las líneas de acción estratégicas de la Ciberseguridad Nacional, al tiempo que se establece la estructura orgánica a su servicio.

Por otro lado, respecto a la primera línea estratégica de acción (Reforzar las capacidades ante las amenazas provenientes del ciberespacio) de la Estrategia de Ciberseguridad Nacional, destaca potenciar y apoyar los desarrollos realizados en la red de CSIRT española (Computer Security Incident Response Team o equipo de Respuesta ante Emergencias Informáticas en español).

A continuación, se presentan algunos centros de respuesta ante incidentes:

1. El CERT (*Computer Emergency Response Team*) de Seguridad e Industria (**CERTSI)**, creado conjuntamente por los Ministerios de Interior e Industria, Energía y Turismo a través de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información. Este CERT tiene su sede en el Instituto Nacional de Tecnologías de la Comunicación (INCIBE). De esta forma, en respuesta a incidentes sobre las tecnologías de la información de las infraestructuras críticas ubicadas en España, INCIBE se convierte en una herramienta de apoyo al CNPIC (Centro Nacional para la Protección de las Infraestructuras Críticas) en la gestión de incidentes de ciberseguridad. Por tanto, el **CERTSI** de **INCIBE** es un CERT de Seguridad e Industria. CERT Nacional competente en la prevención, mitigación y respuesta ante incidentes cibernéticos en el ámbito de las empresas, los ciudadanos y los operadores de infraestructuras críticas.

2. El CCN-CERT del Centro Criptológico Nacional se crea como CERT nacional gubernamental y tiene responsabilidad en ciberataques sobre sistemas de las Administraciones Públicas.

NOTA: REYES es la herramienta del CCN-CERT para el intercambio de información de ciberamenazas. Basado en la tecnología **MISP** (Malware Information Sharing Platform), y especialmente ideado para ofrecer un modo de intercambio de información entre distintas organizaciones que internamente generan ciberinteligencia.

La herramienta de ticketing del CCN-CERT para la gestión de incidentes se llama **LUCIA.**

3. A destacar también el **IRIS-CERT** de RedIRIS tiene como finalidad la detección de problemas que afecten a la seguridad de las redes de centros de RedIRIS. Principalmente orientado a la comunidad científica

Por último, la Unión Europea ha creado mediante el Reglamento (CE) nº 460/2004 del Parlamento Europeo y del Consejo, de 10 de marzo de 2004, la agencia ENISA (Agencia Europea de Seguridad de las Redes y de la Información). Su función principal es la prevención, reacción, gestión y asesoramiento en seguridad y la coordinación entre los países de la Unión.

2 LA SEGURIDAD EN REDES

2.1 DIMENSIONES DE LA SEGURIDAD

Triada CIA (*Confidentiality, Integrity, Availability*) clásica:

- **Confidencialidad:** Propiedad que garantiza que la información llegue solamente a las personas autorizadas e impide la divulgación a otras personas o sistemas no autorizados.

- **Integridad:** Propiedad que mantiene con exactitud los datos originados, sin ser manipulados o alterados por terceros.

- **Disponibilidad:** Disposición de los servicios a ser usados cuando sea necesario por las personas o procesos autorizados en el momento que lo requieran. La carencia de disponibilidad supone una interrupción del servicio.

Como también se puede comprobar en ambas definiciones, a la tradicional Triada CIA, se pueden añadir otras características o propiedades, entre las que destacan:

- **Autenticidad**: Propiedad que permite identificar al generador de la información y así poder asegurar el origen de la información. La identidad del emisor puede ser validada, de modo que se puede demostrar que es quien dice ser.

- **No repudio:** Propiedad que permite probar la participación de las partes en una comunicación. Si la autenticidad prueba quién es el autor de un documento y cuál es su destinatario, el "no repudio" prueba que el autor envió la comunicación
(no repudio en origen) y que el destinatario la recibió (no repudio en destino).

- **Trazabilidad:** capacidad para reconstruir el historial de la utilización o la localización de producto mediante una identificación registrada

NOTA: Esto se ve con más profundidad en el tema de Seguridad en sistemas: Análisis y gestión de riesgos.

2.2 PRINCIPALES PROBLEMAS DE SEGURIDAD EN LAS REDES

Atendiendo a los tres factores de seguridad (Confidencialidad, Integridad, Disponibilidad) analizados en el punto anterior, las amenazas a la seguridad pueden ser clasificadas en cuatros grupos dependiendo del factor de seguridad comprometido:

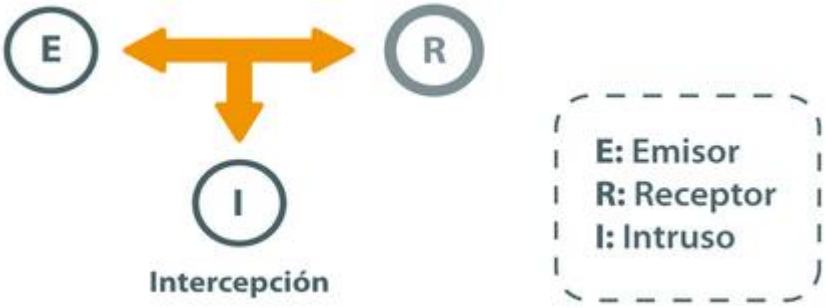
- **Interrupción (afecta a la disponibilidad)**. Se corta el flujo de información entre el emisor y el receptor. El acceso a un recurso/comunicación se ve interrumpido ya sea físicamente (destrucción de la red...) o lógicamente (se modifica la localización, los derechos de acceso...).

- **Intercepción (afecta a la confidencialidad)**. Un elemento no autorizado consigue acceso al sistema y al flujo de información. Alguien no autorizado consigue tener acceso al recurso/comunicación (pinchar la línea de red, sniffing...).

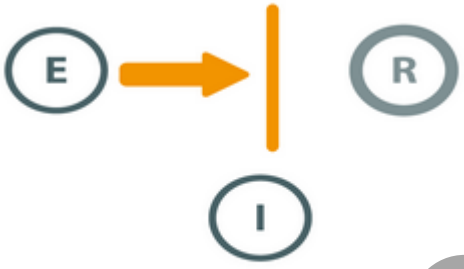
- **Modificación (afecta a la integridad)**. Una entidad consigue cambiar los datos del flujo de información. Obtención no sólo de acceso no autorizado al recurso/comunicación, sino también de la capacidad de modificarlo (modificación de los datos enviados/recibidos entre dos ordenadores...).

- **Fabricación (afecta a la integridad)**. Una entidad inventa y añade datos a los enviados en el flujo de información. Además de conseguir acceso al recurso/comunicación, se tiene la posibilidad de insertar información falsa.

Pregunta de examen A1 2017



Modificación



Interrupción

Fabricación

2.3 TIPOS DE ATAQUES

I *DoS* (Denial of Service). Denegación de servicio.

Ataques que atentan con la disponibilidad de los servicios en red. Básicamente, consisten en saturar mediante peticiones continuadas de servicio, algún servicio de red. Existen muchas modalidades de este tipo de ataques, en función del tipo de nivel de servicio que se desea anular (nivel de enlace, red o aplicación).

- *SYN flodding*. El atacante envía mensaje SYN (synchronize) sin llegar a completar el proceso de conexión y sin enviar el mensaje ACK (aknowlege) final.
- *ICMP flodding*. Consiste en enviar de forma continuada un número elevado de paquetes ICMP de tamaño considerable. Un caso particular de este tipo de ataque es el ***Smurf*** (Ataque pitufo) que

consiste en solicitar un ping falsificado desde la dirección IP del objetivo a una red de broadcast.

Uno antiguo es **Nuke attack**. "*Type of antiquated denial-of-service (DoS) attack carried out by sending fragmented or corrupted (usually ICMP) packets to a target machine. For any machine running an older more vulnerable operating system, sending such packets to it will slow down and eventually stop it, resulting in a crash or Blue Screen of Death (BSoD) in the case of Windows*."

- *UDP flodding*. Se basa en el envío de números paquetes UDP de forma simultánea al equipo atacado.
- ***Teardrop*** (ataque por fragmentación IP): para intentar engañar a firewalls que analizan el nivel 3 sin posibilidad de recomposición de paquetes. Los sistemas más modernos ya no son vulnerables a este tipo de ataque.
- *Buffer overflow*. Se envía más paquetes de los que el buffer puede soportar.

II Ataque distribuido de denegación de servicio DDoS (Distributed Denial of Service).

Los ataques de denegación de servicio son tan antiguos como las máquinas. El ataque DDoS consiste en efectuar una enorme cantidad de peticiones a una computadora o servidor web con el propósito de provocar una sobrecarga de los recursos del sistema informático hasta que la red se ralentiza por los accesos masivos y no pueda satisfacer las solicitudes de usuarios legítimos.

El ataque DDoS utiliza múltiples equipos (esto le diferencia del ataque DoS que se se lleva a cabo en un solo ordenador) contra un único sistema. Si la red de ordenadores atacante es producto de la infección por software malicioso (*botnets*), suele ocurrir que los usuarios legítimos de estos equipos no son conscientes de estar realizando el ataque, lo que siembra ciertas dudas sobre la responsabilidad final de estos usuarios cuyos equipos sirven de atacantes involuntarios.

Como ejemplos de este tipo de ataque destacan:

- Ciberataque de marzo de 2013 contra una organización que se dedicaba al spam, lo que provocó que la velocidad de Internet en todo el mundo fuese reducida por el incidente.
- En julio de 2014, hackers del grupo "*Ciberberkut*" bloquearon con un ataque DDoS durante casi 24 horas la página del presidente de Ucrania, a quien acusaron de genocidio de su pueblo.
- Ataques a proveedores del servicio DNS de tiendas virtuales como Amazon e e-Bay en varias ocasiones en los últimos años. El trastorno económico no sólo

deriva de la ausencia de ventas durante el tiempo de caída por denegación, sino también de la pérdida de confianza de los posibles usuarios.

- En octubre de 2016 un ataque DDoS al proveedor de servicios de DNS DynDNS tumbó servicios de Twitter, Spotify, Paypal, etc.

Soluciones comerciales como Arbor Peakflow se utilizan para mitigar ataques DDoS

Generalmente los ataques DDoS entrarán en una de estas tres categorías:

- **Ataques DDoS volumétricos**
  Intento de consumir el ancho de banda ya sea dentro de la red/servicio objetivo, o entre la red/servicio destino y el resto de Internet.

- **Ataques DDoS de agotamiento de estado TCP**
  Este tipo de ataque DDoS intenta consumir las tablas de estado de conexión que se encuentran en muchos componentes de la infraestructura, como balanceadores de carga, firewalls y los propios servidores de aplicaciones.

- **Ataques DDoS de capa de aplicaciones**
  Este es el tipo más letal de ataque DDoS. Puede ser muy efectivo con tan solo una máquina que ataca y genera una tasa de tráfico baja (esto hace que estos ataques sean muy difíciles de detectar y mitigar proactivamente).

III *Ataque por desbordamiento de buffer (Buffer Overflow).*

Este tipo de ataque se basa en un fallo de programación que se produce por ausencia de control adecuado de la cantidad de datos que se copian sobre un área de memoria reservada a tal efecto (buffer). Asimismo, suelen estar diseñados para activar la ejecución de un código arbitrario al ocurrir esta situación
y conseguir el control de la máquina con los máximos privilegios. Un ejemplo de este ataque es una vulnerabilidad en la librería criptográfica de OpenSSL:

- *Bug Heartbleed.* Las implementaciones de TSL de determinadas versiones de OpenSSL no manejan adecuadamente algunos paquetes construidos específicamente para provocar un desbordamiento de buffer. Esta debilidad reportada en abril de 2014 permite obtener información sensible alojada en la memoria del sistema afectado. Vulnerabilidad muy crítica. Se podían conseguir las claves privadas SSL de un servidor

IV *Ataque de fuzzing*

Fuzzing es una técnica (automatizada o semiautomatizada) de pruebas de software de caja negra que consiste en encontrar “bugs” utilizando inyección de datos

malformados. Esto puede provocar ataques de buffer overflow, denegaciones de servicio o fugas de memoria ("memory leak": error de software que ocurre cuando un bloque de memoria reservada no es liberada en un programa).

V *Ataques de ingeniería social.*

Se trata de explotar la tendencia de los seres humanos a confiar en los demás especialmente en aquellos temas que más desconocemos. El atacante se hace pasar por personal de explotación o del grupo de sistemas para obtener las palabras de paso de los usuarios por teléfono. Otra técnica muy empleada es el "*phising*" que consiste en enviar correos electrónicos que aparentan provenir de fuentes fiables, típicamente bancos.

- **Shoulder surfing.** Mirar por encima del hombro. Intentar conseguir información (contraseñas, pin de la tarjeta de crédito, etc) acercándonos a otra persona.

- **Pretexting / Impersonate:** estas técnicas van de la mano y pueden usarse tanto en los ataques locales como en los remotos. Un claro ejemplo puede darse cuando el atacante se hace pasar por un empleado de soporte técnico de la empresa en la cual trabaja la víctima (impersonate). De esta manera trata de generar empatía para ganar credibilidad, pero acto seguido presenta algún tipo de excusa o pretexto (pretexting), como alertar a la víctima de un comportamiento inadecuado en su equipo, el cual requiere de su intervención. Así podrá dar instrucciones específicas que terminarán en la instalación de algún tipo de malware, concretando así su objetivo (tomar el control del equipo, obtener datos sensibles, etc.).

- **Tailgaiting:** este tipo de ataque se aprovecha de la solidaridad y buena voluntad. Colarse en un sitio diciendo al que va a entrar delante de ti, que te has olvidado la tarjeta.

- **Information diving, dupster diving, trashing**: conseguir información mirando en papeleras, basura, etc. Afecta a la confidencialidad.

- **Distracción Misdirection**. Desviar la atención de la víctima.

- **Baiting:** es una técnica muy efectiva. Generalmente se utilizan pendrives con software malicioso que se dejan en el escritorio de la víctima para que los conecte al PC.

- **Phishing.** Ataque remoto. envío de correos electrónicos conteniendo adjuntos con malware o links a páginas falsas (banca, etc.) con el objetivo de tomar control del

equipo de la víctima o buscando establecer una relación con la mismas (jugando con sus sentimientos).

Esta técnica se convierte aún más peligrosa y efectiva cuando es apuntada a un objetivo específico, como un empleado que tiene acceso a diferentes sistemas dentro de su empresa. En este caso se la conoce como **Spear Phishing**, ya que más que pescar sería cazar con un arpón.

Phising del mundial de fútbol de 2014. A principios de 2014, se recibe este tipo de ataque que consistía en proponer al usuario un enlace hacia un sitio web para ganar entradas para los partidos del mundial de fútbol. El sitio web solicitaba al usuario sus datos personales y bancarios.

- **Whaling.** Técnicas de phishing dirigidas contra objetivos de alta importancia dentro de una organización (altos directivos de empresa, políticos, etc.) o simplemente de gran transcendencia social (cantantes, artistas, famosos, etc.).
- **Vishing** es una práctica fraudulenta que consiste en el uso del Protocolo Voz sobre IP (VoIP).

- **Tabnabbing** Ataque de phishing basado en web, el cual consiste solicitar al usuario sus credenciales de acceso a cuentas de correo electrónico o redes sociales, en páginas web que aparentan ser reales.

- **Redes Sociales**

- **Phreakers (Hackers Telefónicos),**

  Kevin Mitnick, fue quien impulsó e hizo conocido el concepto de Ingeniería Social dentro del mundo de las Tecnologías de la Información. Fue un famoso Phreaker.

  - *"VoIPhreaking"*: hackear, explorar y explotar la infraestructura telefónica de VoIP, a los efectos de realizar llamadas telefónicas gratuitas, en fraude a las compañías telefónicas.
  - VoIPhreaking es en Internet el hermano moderno, más joven, del tradicional "phreaking", que es el término usado para las acciones de hackear, explorar y explotar la infraestructura telefónica convencional (PSTN)

VI *Ataques mediante escuchas de redes*.

El "*sniffing*" es el proceso de interceptación de datos que se está emitiendo en una red no segura y permite escuchas a través de un programa que captura la información de la red (*sniffers*), tarjetas de red en modo promiscuo, (se configura la tarjeta de red para que escuche todo el tráfico que pasa por ella) etc. Habitualmente es utilizado en redes

inalámbricas. En el ejemplo siguiente se muestra como también se puede utilizar para el análisis de mensajes en aplicaciones de uso habitual:

- *"WhatsAppSniffer"*: Mediante un fallo de seguridad en la aplicación de mensajería WhatsApp, se podría obtener los chats de otros terminales si están conectados a la misma red Wi-Fi del atacante.

VII *Ataques basados en la mala administración de los sistemas.*

En varias ocasiones, los atacantes realizan ataques mixtos y aprovechan las vulnerabilidades del software y de la mala administración realizada por la organización. Ejemplos de este tipo de ataque son los acontecidos a los sistemas de información de entidades que deben generar confianza como las Infraestructuras de clave pública (PKI) de los Prestadores de Servicios de Certificación (PSC):

- Diginotar: En julio de 2011, el PSC holandés Diginotar fue atacado y el resultado fue la emisión de más de 500 certificados falsos de sitios web conocidos. En los sistemas de Diginotar, el pirata informático descubre y explota varias vulnerabilidades de seguridad de la autoridad de certificación (CA), como demuestra el análisis forense que encontró software malicioso fácilmente detectado por un antivirus, herramientas de hacking y parte de software sin parchear. Además, el pirata aprovecha la mala administración de los sistemas realizada por la organización debido a la nula separación de los componentes en dominios de seguridad, mala estructuración de la red, inexistente separación de funciones y la ubicación de todos los servidores de la CA en el mismo dominio Windows con contraseña débil de administrador.
- Comodo. En marzo de 2011, se generan certificados SSL sin una correcta verificación en el PSC Comodo. En este caso el hacker no ataca la infraestructura de la CA y la acción se dirige al componente encargado de la verificación de la identidad. Se compromete la Autoridad de Registro (RA) con la obtención del usuario y contraseña.
- Ciberataque a Sony Pictures de 2014.

VIII *Spoofing*. Suplantación de la identidad mediantes medios técnicos (spoofing)

Uso de técnicas de suplantación de la identidad. El atacante suplanta la identidad de otra entidad para poder llevar a cabo una acción que de otra forma no podría realizar. Existen diferentes tipos de Spoofing dependiendo de la tecnología.

NOTA: Más información https://hacking-etico.com/2010/08/26/hablemos-de-spoofing/

- MAC-Spoofing (Suplantación de MAC): Tiene como objeto cambiar la dirección de la interfaz de Control de Acceso al medio (MAC - Media Access Control). La suplantación de la dirección MAC puede permitir que se incumplan las listas de control de acceso a servidores o routers, ocultar un equipo en la red o permitir que se haga pasar por otro.

- IP Spoofing (Suplantación de IP): Sustituir la dirección IP origen por otra IP. Se consigue el envío de paquetes con otra dirección IP de origen. Sirven sobre todo para enmascarar ataques de denegación de servicio.

- DHCP-Spoofing (suplantación del servicio DHCP): El objetivo es crear un servidor DHCP que proporcione configuraciones de red manipuladas, haciendo que los usuarios utilicen tanto el router como los DNS que el atacante quiera.

- ARP Spoofing (suplantación de mensajes ARP). Consiste en enviar mensajes ARP falsos. El objetivo es engañar a los otros sistemas con tramas ARP indicando que el equipo del atacante es el router, por ejemplo. Un caso particular de ARP Spoofing es ARP Poisoning que consiste en enviar tramas erróneas ARP que hagan inútil el uso de la red.

  Prevención con DHCP snooping. Mediante DHCP, el dispositivo de red mantiene un registro de las direcciones MAC (lista blanca) que están conectadas a cada puerto, de modo que rápidamente detecta si se recibe una suplantación ARP. También se evitan ataques de rogue DHCP.
  Otra forma de defenderse contra el ARP Spoofing, es detectarlo. Arpwatch es un programa Unix que escucha respuestas ARP en la red, y envía una notificación vía correo electrónico al administrador de la red, cuando una entrada ARP cambia.

- DNS Spoofing (Manipulación de DNS): Consiste en la suplantación de identidad por nombre de dominio. Consiste en conseguir que resuelva con una dirección IP falsa un cierto nombre DNS o viceversa. El objetivo es que los usuarios visiten sitios Web suplantados (como destinos con malware, un buscados manipulado, sitios de phising, etcétera…).

- Web Spoofing (Suplantación de una página web). Enruta la conexión de una víctima a través de una página falsa hacia otras páginas Web (como si fuera un proxy) con el objetivo de obtener información de dicha víctima.

- Mail Spoofing (Suplantación de la dirección de correo electrónico). Se envía mensajes de correo con la dirección de otras personas o entidades. Esta técnica es usada para *spam*.

- ***MitM* (Man in the middle).** El atacante captura el tráfico entre dos sistemas con posibilidad de modificar e inyectar su propio tráfico. Al equipo destino le envía peticiones simulando ser el equipo solicitante. MitM se emplea típicamente para referirse a manipulaciones activas de los mensajes, más que para denotar intercepción pasiva de la comunicación, pero el ataque MitM puede ser de varios tipos:

  - Eavesdropping. Intercepción de la comunicación. Un atacante escucha pasivamente para obtener información que puede utilizarse posteriormente en un ataque posterior con objeto de suplantar a la entidad.

  - *Replay attack*. Repetición. Consiste en la captura de datos y la retransmisión de estos datos válidos.

Wikipedia: Un ataque de replay o playback (ataque de reproducción o ataque de reinyección, es una forma de ataque de red, en el cual una transmisión de datos válida, es fraudulentamente repetida. Es llevada a cabo por el autor o por un adversario que intercepta la información y la retransmite, posiblemente como parte de un ataque enmascarado.
El intercambio de claves Diffie-Hellman en sus primeras versiones podía ser atacado por un ataque de reinyección, sin embargo, esto puede evitarse con una marca secuencial o una marca de tiempo.

  - *Hijacking*. Secuestro. Técnica de un atacante para robar información con objeto de conseguir una conexión de red (*IP hjjacking*), una sesión (*session hijacking*) o una página web (*page hijacking*).

IX *Ataques de Ransomware*
Malware que se transmite como un troyano o un gusano y restringe el acceso a determinadas partes o archivos del sistema infectado, y pide un rescate a cambio de quitar esta restricción.

Algunos tipos de ransomware cifran los archivos del sistema operativo inutilizando el dispositivo y coaccionando al usuario a pagar el rescate. El correo es el origen como ataques de phishing, pero hay otras muchas opciones.

Ejemplos:

- **Cryptolocker:** Ataque más popular. La mayoría de los ataques de ransomware son ataques evolucionados de cryptolocker.
- **SamSam** *"In 2016, a new strain of ransomware emerged that was targeting JBoss servers.[103] This strain, named "SamSam", was found to bypass the process of phishing or illicit downloads in favor of exploiting vulnerabilities on weak servers."*
- **Jigsaw** *"is a form of encrypting ransomware malware created in 2016."*
- **Hitler-Ransomware** *"was first developed in 2016. The ransomware activates with a lock screen with an image of Adolf Hitler giving a Nazi salute."*
- **Wannacry**: mayo 2017. Usaba la vulnerabilidad **EternalBlue** (CVE-2017-0144) desarrollada por la NSA (Agencia de Seguridad Nacional de los Estados Unidos) para propagarse:
  CVE-2017-0144 en el catálogo Common Vulnerabilities and Exposures (CVE), se debe a que la versión 1 del servidor **SMB** (SMBv1) acepta en varias versiones de Microsoft Windows paquetes específicos de atacantes remotos, permitiéndoles ejecutar código en el ordenador en cuestión.
- **Petya** Junio2017 Este malware utiliza ingeniería social para convencer a usuarios (o a administradores de redes) de descargar un archivo que al abrirlo se autoextrae y ejecuta el troyano.
- *"On 24 October 2017, some users in Russia and Ukraine reported a new ransomware attack, named **"Bad Rabbit",** which follows a similar pattern to WannaCry and Petya by encrypting the user's file tables and then demands a BitCoin payment to decrypt them"*
- **BitPaymer/iEncrypt y Ryuk** dirigidos a grandes empresas.

X *APTs*

En la actualidad uno de los ataques específicos más conocidos son los APT (**Amenaza persistente avanzada).** Son ataques dirigidos destinados a penetrar la seguridad informática de una entidad específica. El término avanzado hace referencia al uso de técnicas sofisticadas para explotar vulnerabilidades. Hacen uso de ingeniería social, vulnerabilidades, etc. Son persistentes porque a través de un control externo van extrayendo información de forma continua.

NOTA: La herramienta **CARMEN** del CCN-CERT está diseñada para la detección de APTs en las organizaciones.

XI *Ataques sobre criptomonedas*

- **'Ataque 51%'**. Los mineros de criptomonedas pueden convertirse en la mayor amenaza para su red llevando a cabo este ataque. Un **ataque 51% se da en la tecnología blockchain**, como la de Bitcoin, cuando una sola persona o grupo de minado toman el control de un 51% del poder computacional de de la red.

- "Minería forzada" a través de la cual los delincuentes cibernéticos insertan líneas de código en sitios web vulnerables, correos electrónicos o descargas que se ejecutan en la computadora del usuario y secuestran su equipo para minar criptomonedas en nombre del atacante.

- **Coinhive**. Malware usado para minar criptomonedas.

https://hipertextual.com/2018/01/que-es-coinhive-malware-minar-criptomonedas

XII *Ataques populares en 2019*

- Malware EMOTET https://es.malwarebytes.com/emotet/
- GINP troyano bancario en Android.

2.4 REDES INALÁMBRICAS

Al no requerir conexión física, el atacante simplemente debe estar dentro del perímetro de la red inalámbrica y, con un acceso no autorizado, podría escanear y obtener todos los datos que se transmiten a través de la red. Las consecuencias serían desde la reducción del ancho de banda hasta el acceso a nuestra información personal, contraseñas, etc. NIST ha dedicado una publicación especial, SP 800-153 - *Guidelines for Securing Wireless Local Area Networks*

(WLANs) con las recomendaciones de seguridad en las redes de área local inalámbricas.

Respecto a la seguridad en redes WIFI, varios aspectos deben ser tenidos en cuenta:

- **Configuración inadecuada**. Mantener la configuración por defecto del router o mal configurado permitirá la labor de conexión ilícita a la red WiFi

- **Sistema de Cifrado incorrecto.** Utilizar un sistema de cifrado WEP (*Wired Equivalent Privacy*) o WPA (*Wi-FI Protected Access*) no son opciones adecuadas.

- **Clave no robusta.** Incluso un cifrado WPA-2 con AES puede ser vulnerable con una clave débil. Una contraseña fuerte complica la probabilidad de "romper" la contraseña mediante la fuerza bruta.

- **Sistemas de control y detención.** La instalación de sistemas de detección (IDS) y cortafuegos con objeto de detectar accesos no autorizados y restringir los accesos.

Wardriving: búsqueda de redes inalámbricas Wi-Fi desde un vehículo en movimiento. Implica usar un coche o camioneta y un ordenador equipado con Wi-Fi, como un portátil o una PDA, para detectar las redes.

NOTA: Más información sobre seguridad en redes inalámbricas en la guía CCN-STIC-406**.**

2.5 LA SEGURIDAD EN LAS REDES Y EL SOFTWARE LIBRE

Existen diversas soluciones de seguridad en software libre y que pueden ser consideradas como una alternativa a programas de software. Desde análisis del tráfico de red en busca de tráfico inusual o malicioso Wireshark, firewalls (iptables), sistemas de detección de intrusión (por ejemplo, Snort), escáneres de vulnerabilidad (como Nessus), antivirus (ClamAV), entre otros.

3 CONTROL DE ACCESOS

3.1 ACCESO, AUTENTICACIÓN E IDENTIFICACIÓN.

El control de accesos es el método por el cual se incrementa la seguridad de una red mediante la restricción de uso de los recursos a los usuarios de la red de acuerdo con una política de seguridad definida. Para permitir el acceso, es fundamental conocer si el usuario o máquina se encuentra dentro de los grupos permitidos en la política de seguridad.

Este control de accesos se implementa habitualmente en diferentes niveles:

- Aplicación
- Middleware
- Sistema Operativo
- Hardware

Existen dos tipos de políticas de control de acceso:

NOTA: Esta parte es muy teórica y poco probable de ser preguntada en el test.

- **Modelo de control de acceso discrecional** (DAC): el propietario de un recurso es un usuario identificado que decide discrecionalmente qué otros sujetos podrán acceder al citado recurso. Se puede transferir la propiedad, así como delegar la concesión de permisos. No obstante, este modelo tiene el problema llamado "caballo de Troya" derivado de su carácter discrecional, donde un tercero podría acceder a un recurso sin estar autorizado. Se precisa por tanto introducir el concepto de seguridad multinivel y multilateral.

- **Modelo de control de acceso no discrecional o mandatorio** (MAC): el sistema protege los recursos. Los objetos y sujetos están compartimentados, a través de etiquetas de seguridad. El sistema permite el acceso a recursos si y sólo si el sujeto tiene el permiso adecuado, comparando las etiquetas del que accede frente al recurso accedido, siguiendo un modelo matemático multinivel (MLS), por ejemplo, Bell-LaPadula, Biba o Clark-Wilson. Los criterios de seguridad TCSEC (Trusted Computer System Evaluation Criteria (TCSEC) is a United States Government Department of Defense (DoD) standard that sets basic requirements for assessing the effectiveness of computer security controls built into a computer system) correspondientes al nivel de seguridad B1 o superior incluyen este modelo.

Wikipedia: El modelo de seguridad Bell-Lapadula consiste en dividir el permiso de acceso de los usuarios a la información en función de etiquetas de seguridad. Por ejemplo, en sistemas militares norteamericanos, categorizándola en 4 niveles: no clasificado, confidencial, secreto y ultrasecreto.

Modelo matemático. Define 2 reglas de control de acceso mandatorio (MAC) y una regla de control de acceso discrecional (DAC) con 3 propiedades:

- Propiedad de seguridad simple: Un sujeto de un determinado nivel de seguridad no puede leer un objeto perteneciente a un nivel de seguridad más alto.
- Propiedad (Propiedad estrella): Un sujeto de un determinado nivel de seguridad no puede escribir un objeto perteneciente a un nivel de seguridad más bajo. (También llamada propiedad de confinamiento).
- Propiedad de seguridad discrecional: Se utiliza una matriz de acceso para especificar el control de acceso discrecional.

Con Bell-La Padula, los usuarios pueden **crear** contenido **sólo en su nivel de seguridad o por encima** (i.e, investigadores en el nivel secreto pueden crear archivos secretos o super secretos, pero no archivos públicos). Inversamente, los usuarios pueden **ver** solamente contenido de su **propio nivel o inferior**.

- Bell-lapadula Este modelo se centra en la confidencialidad y no en la integridad
- Modelo de BIBA se centra en la integridad.

Los modelos DAC y MAC son inadecuados para cubrir las necesidades de la mayor parte de las organizaciones. El modelo DAC es demasiado débil para controlar el acceso a los recursos de información de forma efectiva, en tanto que el MAC es demasiado rígido. Desde los 80 se ha propuesto el modelo de control de accesos basado en roles (RBAC), como intento de unificar los modelos clásicos DAC y MAC, consiguiendo un sistema donde el sistema impone el control de accesos, pero sin las restricciones rígidas impuestas por las etiquetas de seguridad.

En los sistemas distribuidos, es necesario controlar no sólo los usuarios que acceden a los servicios sino también los recursos que ha utilizado. Es importante supervisar quién puede acceder a la red, pero también es importante definir lo que puede hacer y observar las acciones que realice mientras accede. Por esta razón, se utiliza una arquitectura denominada triple-A o AAA (*Authentication, Authorization and Accounting*) para realizar tres funciones con este objeto: autenticación, autorización y trazabilidad (o auditoría).

- **Autenticación**: verificar, mediante alguno de los mecanismos disponibles, que el sujeto se corresponde con la identidad supuesta. El usuario se da a conocer en el sistema y muestra su identidad (identificación). Por su parte, el sistema realiza una verificación sobre esta identificación y comprueba la identidad del usuario (autenticación).

- **Autorización**: cuando un usuario, una vez autenticado, solicita un recurso, se debe comprobar si ese usuario está autorizado. Es decir, puede ser que el usuario no tenga permiso para acceder a un recurso concreto de red. El usuario ya está autenticado pero lo servicios de autorización determinan a qué recursos puede acceder y qué operaciones quedan habilitadas.

- **Trazabilidad** (o auditoría). Registro de toda la actividad que realiza el usuario y de todas las autorizaciones concedidas. El sistema realiza un seguimiento de la forma en que se utilizan los recursos.

3.2 MÉTODOS Y FACTORES DE AUTENTICACIÓN

En función del procedimiento o información utilizada por el sistema para la verificación de la identidad de una entidad, los métodos se pueden clasificar en varias categorías, dependiendo del factor de autenticación usado:

- Sistemas basados en el **"*factor de conocimiento*"** (algo que el usuario sabe). Se trata de algo que el usuario conoce. Es el caso común de las contraseñas, preguntas para recordar contraseñas, PIN…

- Sistemas basados en el **"*factor de posesión*"** (algo que el usuario tiene). Se refiere a un elemento que el usuario posee. Por ejemplo, el uso de tarjetas criptográficas o los *tokens* digitales, donde un usuario presenta un elemento considerado como único, que le permite el acceso al sistema. Son similares a la posesión de una llave.

- Sistemas basados en el **"*factor de inherencia*"** (algo que el usuario es). Se refiere a rasgos intrínsecos del usuario. Aquí entran todos los mecanismos biométricos, desde examen de iris, huellas dactilares o reconocimiento facial. Se diferencian entre los mecanismos fisiológicos (iris, facial,) y los de conducta (voz, tipo de escritura en teclado,).

Se debe tener en cuenta que ISO 19790 «Requisitos de Seguridad para Módulos Criptográficos», define un cuarto "***factor de conducta***" (algo que el usuario suele hacer).

Se habla de **autenticación fuerte** cuando un sistema de autenticación utiliza **por lo menos dos** de los tres factores citados anteriormente. De este modo, si uno de los factores se ve comprometido, todavía existe un segundo factor que garantiza la seguridad.

3.2.1 CONTRASEÑAS

Se utiliza información secreta y compartida para controlar el acceso. Para intentar mejorar sus características de seguridad, los sistemas de control de acceso además implementan:

- Cambio de contraseñas con periodicidad.
- Chequeo de complejidad mínima. Longitud mínima y mezcla de caracteres.
- Teclados cambiantes para la inserción de las contraseñas.

En usuario tiene responsabilidad sobre la fortaleza de la contraseña. Se debe generar una contraseña lo suficientemente larga y con el máximo de caracteres al azar. Passphrase o frase de contraseña son las más seguras.

3.2.2 OTP (ONE TIME PASSWORD)

OTP es una contraseña que sólo puede utilizarse una vez, en una única sesión y posteriormente deja de tener validez. De esta forma, se resta efectividad a los ataques de fuerza bruta y los de repetición (replay).
CL@VE PIN es un OTP.

3.2.3 CERTIFICADOS DIGITALES

Los certificados digitales, basados en la posesión de una clave privada que garantiza la identidad mostrada en el certificado, sirven para la identificación y autenticación de los usuarios. Existen muchas formas de almacenar tanto los certificados como las claves privadas, pero los sistemas que garantizan que la clave no se extraiga son las tarjetas criptográficas y los tokens.

3.2.4 TARJETAS INTELIGENTES (SMARTCARDS)

Estos sistemas tienen chips criptográficos que permiten realizar las funciones criptográficas dentro del dispositivo, sin que la clave privada salga del elemento para

efectuar las funciones de autenticación. Existen varios tipos de clasificación de las tarjetas:

- Según su estructura:
    - Memoria: Funciona como un simple almacén de información.
    - Microprocesador: posee un pequeño computador interno, con las microinstrucciones escritas en ROM.
    - Criptográficas: las más avanzadas, con un microprocesador y un coprocesador matemático para efectuar algoritmos de cifrado.
- Según el interfaz:
    - Tarjetas de contacto. Deben ser insertadas en un lector. Existe un caso particular, Token USB, que se conecta al puerto USB.
    - Tarjeta sin contacto. También denominadas *contactless*. Contienen un chip RFID (*Radio Frequency IDentification*) que permite una identificación por radiofrecuencia a través de la antena interna de la tarjeta.
    - Tarjeta dual. Es una tarjeta de contacto a la que se añadido un segundo chip sin contacto.

3.2.5 BIOMÉTRICOS

Existen, con diferente fiabilidad, sistemas de autenticación biométrica sobre:

- Huellas dactilares.
- Reconocimiento de retina.
- Reconocimiento facial.
- Voz.
- Aliento.
- Escritura.

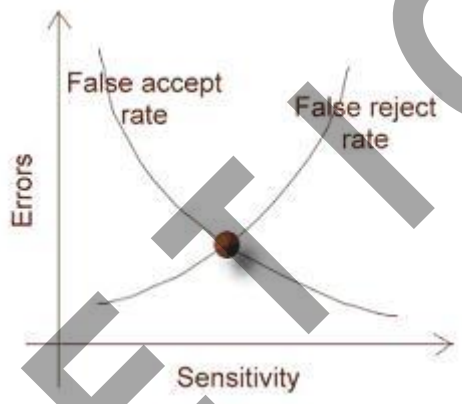
Fuente Wikipedia:

Tabla comparativa de sistemas biométricos. Se puede ver, por ejemplo, que los sistemas biométricos de Iris o Retina son más seguros que los de huella dactilar o reconocimiento de voz.

	Ojo (Iris)	Ojo (Retina)	Huellas dactilares	Vascular dedo	Vascular mano	Geometría de la mano	Escritura y firma	Voz	Cara 2D	Cara 3D
Fiabilidad	Muy alta	Muy Alta	Muy Alta	Muy Alta	Muy Alta	Alta	Media	Alta	Media	Alta
Facilidad de uso	Media	Baja	Alta	Muy Alta	Muy Alta	Alta	Alta	Alta	Alta	Alta
Prevención de ataques	Muy alta	Muy Alta	Alta	Muy Alta	Muy Alta	Alta	Media	Media	Media	Alta
Aceptación	Media	Baja	Alta	Alta	Alta	Alta	Muy Alta	Alta	Muy alta	Muy alta
Estabilidad	Alta	Alta	Alta	Alta	Alta	Media	Baja	Media	Media	Alta

Pregunta examen A1 2017

El rendimiento de una medida biométrica se define generalmente en términos de tasa de falso positivo (False Acceptance Rate o FAR), la tasa de falso negativo (False NonMatch Rate o FNMR, también False Rejection Rate o FRR), y la tasa de fallo de alistamiento (Failure-to-enroll Rate, FTE o FER).



En los sistemas biométricos reales el FAR y el FRR puede transformarse en los demás cambiando cierto parámetro. Una de las medidas más comunes de los sistemas biométricos reales es la tasa en la que el ajuste en el cual acepta y rechaza los errores es igual: la tasa de error igual (Equal Error Rate o EER), también conocida como la tasa de error de cruce (Cross-over Error Rate o CER). Cuanto más bajo es el EER o el CER, se considera que el sistema es más exacto.

BIOMETRÍA CANCELABLE Pregunta examen A1 2017

Uno de los puntos clave de la identificación biométrica es que **las plantillas biométricas no pueden actualizarse o renovarse**; si se descubre una contraseña podrá generarse una nueva de entre infinitas posibles; sin embargo, cada individuo sólo tiene 10 dedos, 2 ojos y 2 orejas. Las tecnologías que protegen a las plantillas biométricas se llaman **Protección de Plantillas biométricas**. Como las características biométricas son inmutables, cuando se roba una plantilla biométrica esa característica queda expuesta para siempre. Sin embargo, la Biometría Cancelable permite revocar una plantilla biométrica comprometida, como si fuera una contraseña perdida.

La **Biometría Cancelable** consiste en proveer una distorsión intencional, sistemática y repetible para proteger los datos sensibles del usuario. Por ejemplo, si se roba una característica "cancelable", las distorsiones provistas se modifican y se remapean en una nueva plantilla que reemplazará a la que haya resultado expuesta. La ventaja de la "biometría cancelable" es que protege la privacidad del usuario, ya que los datos biométricos reales no se revelan durante la autenticación. La distorsión provista, evidentemente, debe ser inadvertible, pues es necesario evitar que se puedan recomponer los datos biométricos originales a partir de los que fueron modificados.

¿Qué es mejor, tecnologías biométricas o una contraseña?

a biometría se basa en la medición de ciertas características únicas del cuerpo humano. Esta es su fortaleza y su debilidad. Si una contraseña resulta robada, puede ser rápidamente reemplazada por una nueva, mientras que, si los datos biométricos son robados, un individuo no puede modificar sus huellas dactilares o su iris.

Las contraseñas y la biometría no están reñidos, de hecho, pueden complementarse.

3.3 PROTOCOLOS DE ACCESO Y AUTENTICACIÓN

Existen diferentes protocolos ya definidos, que se comentan a continuación.

3.3.1 PROTOCOLOS DE AUTENTICACIÓN PPP (POINT TO POINT PROTOCOL)

El protocolo PPP permite establecer una comunicación a nivel de la capa de enlace TCP/IP.

- **PAP (Password Authentication Protocol)**

  Utiliza contraseñas en texto simple y es el protocolo de autenticación menos seguro. Sólo se utiliza cuando el cliente y el servidor no pueden negociar una validación más segura.

- **CHAP (Challenge Handshake Authentication Protocol)**

  CHAP es un protocolo de autenticación de desafío/respuesta. Utiliza MD-5 para calcular un valor que sólo conocen el sistema de autenticación y el dispositivo. Microsoft ha implementado el CHAP en su propio protocolo MS-CHAP. No es seguro.
  CHAP protege contra los ataques de REPLAY mediante el uso de un identificador que se va incrementando y un valor de verificación variable.

- **EAP (Extended Authentication Protocol)**

EAP, recogido en RFC 5247, es un marco de autenticación, no un mecanismo realmente. Ofrece una estructura de mensajes, que luego se encapsulan dependiendo del protocolo de enlace. Dentro de EAP se pueden utilizar los mecanismos (de cifrado, por ejemplo) que se deseen. Permite el negociado del mecanismo de autenticación, y a este negociado se le conoce como métodos. Existen unos 40 métodos, de los que merece la pena destacar:
EAP es un framework de autenticación

- ***Lightweight Extensible Authentication Protocol (LEAP)***: sistema inicial, creado por CISCO en el que las credenciales del usuario no se consideran protegidas suficientemente.

- ***EAP Pre-Shared Key (PSK)***: permite la autenticación cuando ambas partes comparten una clave. Si la clave es compartida por varios usuarios puede constituir una debilidad.

- ***EAP - Transport Layer Security (EAP-TLS)***: utiliza TLS (anteriormente conocido como SSL) para las comunicaciones. Permite la autenticación de usuario y de servidor mediante PKI. La única desventaja es la sobrecarga al utilizar certificados en ambas partes.

- ***EAP - Tunneled Transport Layer Security (EAP-TTLS)***: mejora EAP-TLS en cuanto que no requiere autenticación del usuario por certificados, si bien no está soportado de forma nativa por la mayoría de los sistemas operativos.

- ***EAP - IKEv2***, basado en Internet Key Exchange Protocol version 2 (IKEv2), permite diferentes configuraciones de mecanismos, desde claves asimétricas, contraseñas y claves simétricas, a escoger por el servidor o por el usuario.

- ***Protected Extensible Authentication Protocol (PEAP)***, desarrollado por Cisco, Microsoft y RSA Security como estándar abierto. Es similar a EAP-TTLS, ya que requiere únicamente el certificado de servidor.

- **EAP-FAST** (Flexible Authentication via Secure Tunneling) fue desarrollado por Cisco. *"The EAP-FAST protocol is a client-server security architecture that encrypts EAP transactions with a Transport Level Security (TLS) tunnel. EAP-FAST tunnel establishment is based on strong*

secrets that are unique to users. These strong secrets are called PACs, which the ACS generates by using a master key known only to the ACS."

3.3.2 PROTOCOLOS DE AUTENTICACIÓN AAA (AUTHENTICATION, AUTHORIZATION AND ACCOUNTING)

Como ya se ha comentado anteriormente, estos protocolos se caracterizan por la prestación de servicios de autenticación, autorización y auditoría (trazabilidad).

- **Remote Authentication Dial In User Service (RADIUS)**

  Es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP. Permite la transmisión de credenciales. La máquina que realiza todas las comprobaciones de credenciales se llama "RADIUS Server". Utiliza UDP para establecer las conexiones. El servidor RADIUS comprueba que la información es correcta utilizando esquemas de autenticación como PAP, CHAP o EAP.
  RADIUS es capaz de manejar sesiones, notificando cuándo comienza y termina una conexión, así que al usuario se le podrá determinar su consumo y facturar en consecuencia; los datos se pueden utilizar con propósitos estadísticos

- **TACACS+ (Terminal Access Controller Access Control)**

  Desarrollo por CISCO. Es un protocolo de autenticación remota. Es similar a RADIUS, pero con la diferencia de que TACACS utiliza TCP. Se ha publicado una descripción del protocolo en IETF RFC 1492. Actualmente todavía se usa, pero de forma residual.

- **DIAMETER**

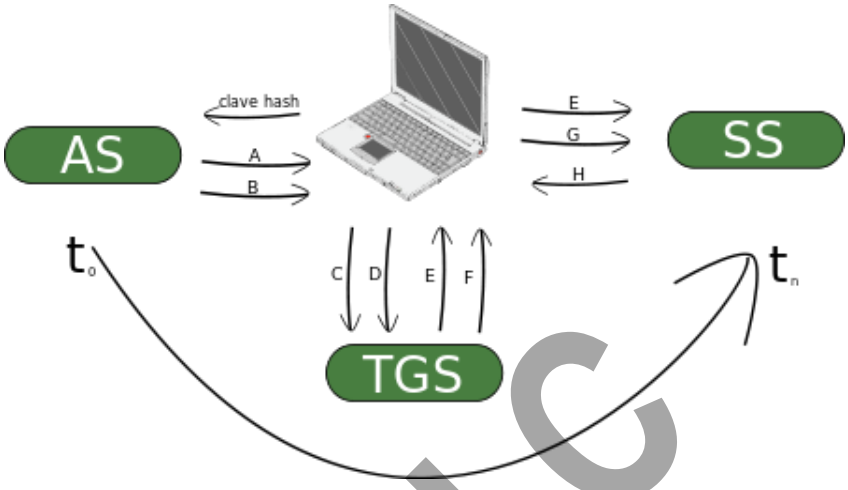
  Es un protocolo basado en el mismo concepto que RADIUS. El objetivo de DIAMETER es proporcionar un protocolo base que pueda ser extendido para proporcionar servicios AAA a nuevas tecnologías de acceso más complejas y seguras requeridas por la actual generación de IP móvil y redes inalámbricas. **Utiliza TCP**

- **Kerberos**

  Kerberos es un protocolo de autenticación mediante tickets. El sistema **se basa en criptología de clave simétrica** y utiliza un denominado tercero de confianza denominado Key Distribution Center (KDC). El usuario se

autentica en un servidor de autenticación, que le entrega un ticket que luego muestra a los diferentes recursos para hacer uso de ellos.

"Kerberos builds on symmetric key cryptography and requires a trusted third party, and optionally may use public-key cryptography during certain phases of authentication. Kerberos uses UDP port 88 by default."



Creado por el MIT

El KDC está formado por un servidor de autenticación AS y un servidor emisor de tickets TGS

Otro proyecto del MIT no muy usado es **Athena**.

3.3.3 AUTENTICACIÓN EN LA CAPA IP: IPSEC

- IPsec (Internet Protocol Security) es un **conjunto de protocolos** cuya función es **asegurar las comunicaciones sobre el Protocolo de Internet** (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos. IPsec **también incluye protocolos para el establecimiento de claves de cifrado.**

- Los protocolos de IPsec **actúan en la capa de red**, la capa 3 del modelo OSI.

- Esto hace que IPsec sea **más flexible**, ya que puede ser utilizado para proteger protocolos de la capa 4, incluyendo TCP y UDP, los protocolos de capa de transporte más usados.

- Una ventaja importante de IPsec frente a SSL y otros métodos que operan en capas superiores, es que **para que una aplicación pueda usar IPsec no hay que hacer ningún cambio**, **mientras que, para usar SSL y otros protocolos de niveles superiores, las aplicaciones tienen que modificar su código**.

- IPsec es una parte **obligatoria de IPv6**, y su uso **es opcional con IPv4**.

- IPSec puede ser **implementado bien en un host o bien en un equipo dedicado**, tal como un router o un firewall, que cuando realiza estas funciones se denomina gateway IPSec.

- Como el IP no provee intrínsecamente de ninguna capacidad de seguridad, IPsec se introdujo **para proporcionar servicios de seguridad** tales como:

    - **Cifrar el tráfico**.
    - **Validación de integridad**.
    - **Autenticar a los extremos**.
    - **Anti-repetición** (proteger contra la repetición de la sesión segura).

- Los **algoritmos criptográficos** definidos para usar con IPsec incluyen HMAC y SHA-1 para protección de integridad, y Triple DES-CBC y AES-CBC de 128 bits para confidencialidad. Más detalles en la RFC 4305.

- La arquitectura de seguridad IP utiliza el concepto de **Asociación de Seguridad** (SA) como base para construir funciones de seguridad en IP.

- Una asociación de seguridad es simplemente el paquete de algoritmos y parámetros (tales como las claves) que se está usando para cifrar y autenticar un flujo particular en una dirección.

- Por lo tanto, en el tráfico normal bidireccional, **los flujos son asegurados por un par de asociaciones de seguridad**. La decisión final de los algoritmos de cifrado y autenticación (de una lista definida) le corresponde al administrador de IPsec.

- Para decidir qué protección se va a proporcionar a un paquete saliente, IPsec utiliza el **índice de parámetro de seguridad (SPI)**, un índice a la base de datos de asociaciones de seguridad (SADB), junto con la dirección de destino de la cabecera del paquete, que juntos identifican de forma única una asociación de seguridad para dicho paquete. Para un paquete entrante se realiza un procedimiento similar; en este caso IPsec toma las claves de verificación y descifrado de la base de datos de asociaciones de seguridad.

- IPsec consta de los siguientes **protocolos**:

    - **Protocolos de Seguridad.**
        - **Authentication Header (AH).**
        - **Encapsulating Security Payload (ESP).**

    - **Protocolos de gestión de claves.**
        - **Internet Key Exchange (IKE).**

- **AH (Authentication Header).**

    - Proporciona: **Integridad, Autenticación, No repudio** (si se eligen los algoritmos criptográficos apropiados).

- **No ofrece confidencialidad.**

- AH está dirigido a garantizar integridad sin conexión y autenticación de los datos de origen de los datagramas IP. Para ello, calcula un Hash Message Authentication Code (HMAC) a través de algún algoritmo hash operando sobre:

  - Una clave secreta.
  - El contenido del paquete IP.
  - Las partes inmutables del datagrama.

- Lo que se obtiene como resultado del HMAC es una cadena de caracteres llamada extracto (huella). El emisor calcula un extracto del mensaje original, que se copia en uno de los campos de la cabecera AH

- Este proceso restringe la posibilidad de emplear NAT, que puede ser implementada con NAT traversal NAT-T

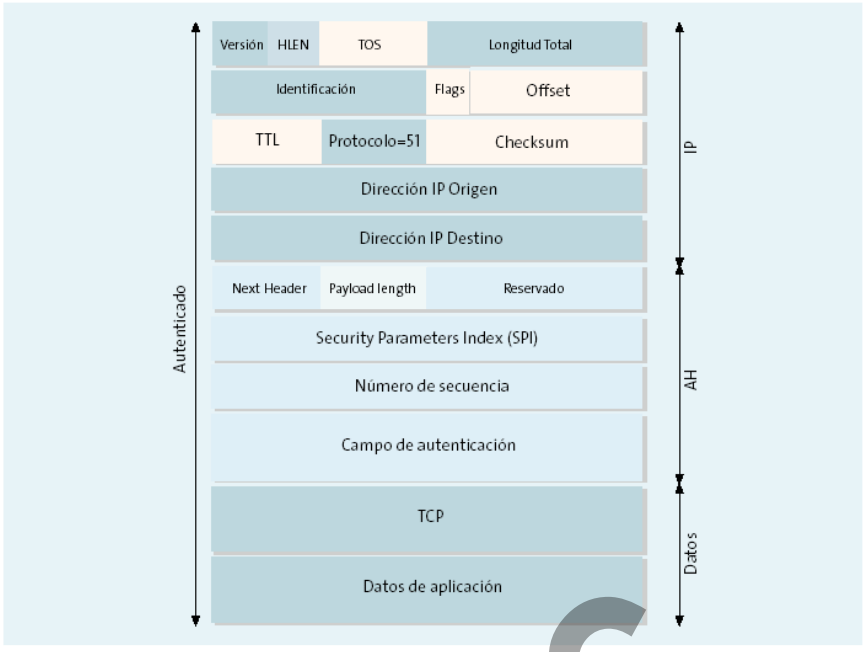
- La seguridad de AH reside, por tanto, en el cálculo del extracto MAC, imposible sin conocer la clave, y que dicha clave sólo la conozcan emisor y receptor.

- AH protege la carga útil IP y todos los campos de la cabecera de un datagrama IP excepto los campos mutantes, es decir, aquellos que pueden ser alterados en el tránsito. En IPv4, los campos de la cabecera IP mutantes (y por lo tanto no autenticados) incluyen TOS, Flags, Offset de fragmentos, TTL y suma de verificación de la cabecera.

- AH opera directamente por encima de IP, utilizando el protocolo IP número 51. En el campo protocolo de la cabecera IP aparecerá “51” y dentro de la cabecera AH es donde se identifica el tipo de datos de la capa superior.

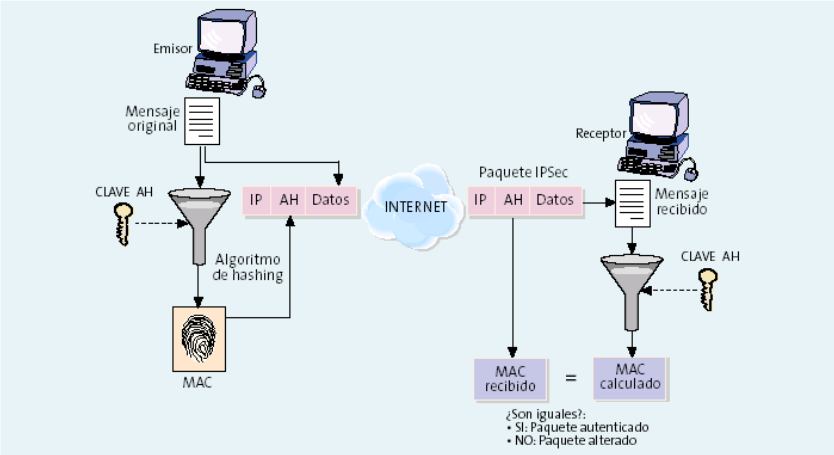
- Lo que se hace es que se inserta una cabecera AH entre la cabecera IP estándar y los datos transportados (que pueden ser TCP, UDP, ICMP o un datagrama IP completo).

- Una Cabecera AH mide 32 bits, he aquí un diagrama de cómo se organizan:
  - Next header: identifica el protocolo de los datos transferidos.
  - Payload length: tamaño del paquete AH.
  - Security parameters index (SPI): indica los parámetros de seguridad que, en combinación con la dirección IP, identifican la asociación de seguridad implementada con este paquete.
  - Sequence number: un número siempre creciente, utilizado para evitar ataques de repetición.
  - HMAC: contiene el valor de verificación de integridad (ICV) necesario para autenticar el paquete; puede contener relleno.



AH protege la carga útil IP y todos los campos de la cabecera de un datagrama IP excepto los campos mutantes, es decir, aquellos que pueden ser alterados en el tránsito. En IPv4, los campos de la cabecera IP mutantes (y por lo tanto no autenticados) incluyen TOS, Flags, Offset de fragmentos, TTL y suma de verificación de la cabecera.

0 - 7 bit	8 - 15 bit	16 - 23 bit	24 - 31 bit
Next header	Payload length	RESERVED	
Security parameters index (SPI)			
Sequence number			
Hash Message Authentication Code (variable)			



- **ESP (Encapsulating Security Payload).**

  - Proporciona: **Confidencialidad y, opcionalmente, Autenticidad de origen, Integridad**.

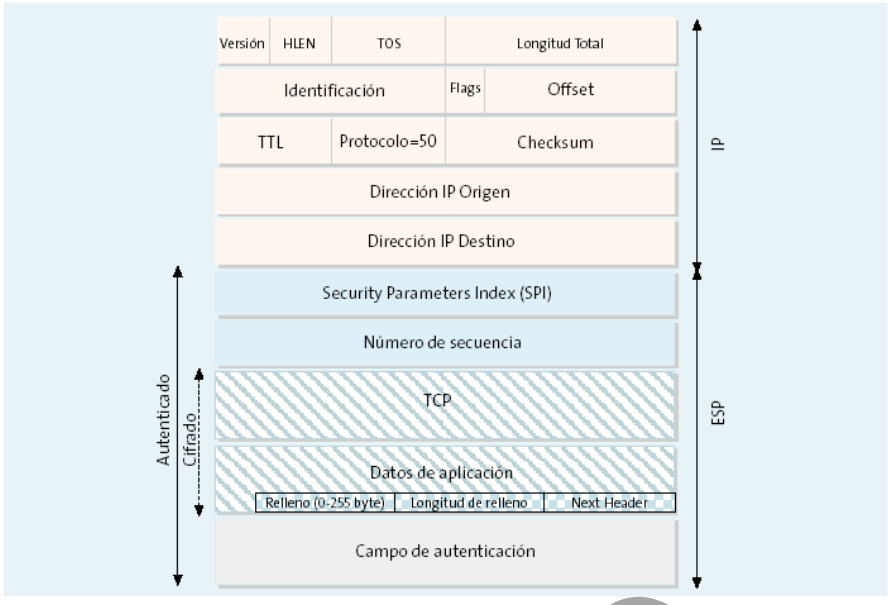
  - Al contrario que con AH, la cabecera del paquete IP no está protegida por ESP (aunque en ESP en modo túnel, la protección es proporcionada a todo el paquete IP interno, incluyendo la cabecera interna; la cabecera externa permanece sin proteger).

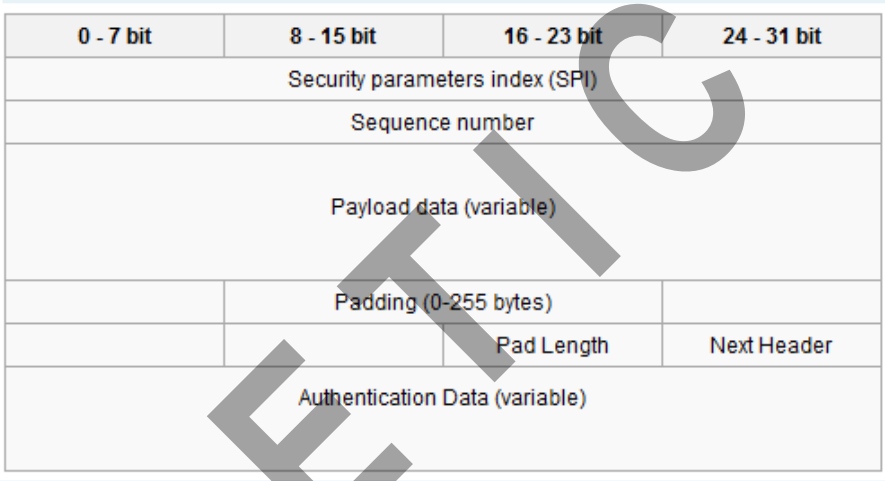
  - ESP opera directamente sobre IP, utilizando el protocolo IP número 50. Ese será el valor del campo protocolo y dentro del mensaje ESP se indicará la naturaleza de los datos.

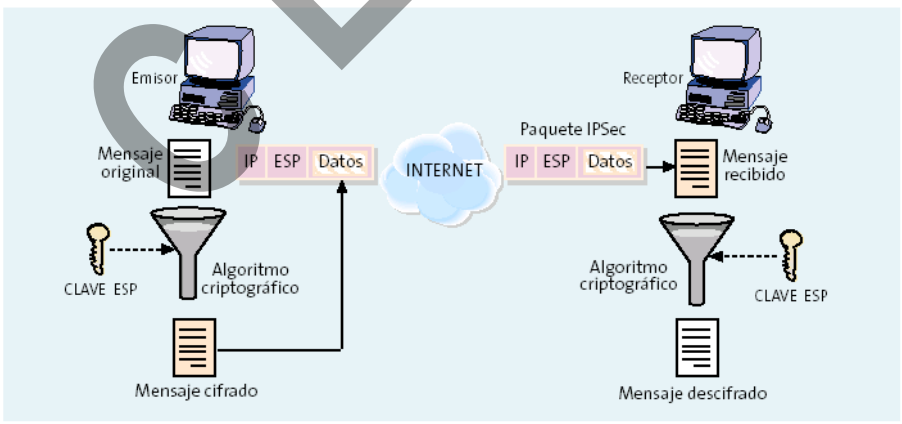
  - Como ofrece más funcionalidades que AH, la cabecera ESP es más compleja. Este formato consta de una cabecera y una cola que rodean los datos transportados. Dichos datos pueden ser cualquier protocolo IP (por ejemplo, TCP, UDP o ICMP, o incluso un paquete IP completo). En la figura se muestra la estructura de un datagrama ESP, en la que se observa cómo el contenido o carga útil viaja cifrado.

  - El detalle de la cabecera ESP es:

    - Security parameters index (SPI): parámetros de seguridad en combinación con la dirección IP.
    - Sequence number: un número siempre creciente, utilizado para evitar ataques de repetición.
    - Payload data: los datos a transferir.
    - Padding: usado por algunos algoritmos criptográficos para rellenar por completo los bloques.
    - Pad length: tamaño del relleno en bytes.
    - Next header: identifica el protocolo de los datos transferidos.
    - Authentication data: contiene los datos utilizados para autenticar el paquete.







- **IKE (Internet Key Exchange).**

  - Este protocolo crea la llamada SA (Security Association). Esta SA consta de los protocolos y algoritmos para generar las claves temporales usadas por IPSEC. Una vez que se ha realizado esta fase, ambas partes conocen todos los parámetros de la SA.

- **Modos de IPSEC**.

  - **Modo Transporte**.

    - En modo transporte, sólo se cifra o autentica la carga útil (los datos que se transfieren) del paquete IP. Es decir, el contenido transportado dentro del diagrama AH o ESP son datos de la capa de transporte (por ejemplo, TCP o UDP). Por tanto, la cabecera IPSec se inserta inmediatamente a continuación de la cabecera IP y antes de los datos de los niveles superiores que se desean proteger.

    - El enrutamiento permanece intacto, ya que no se modifica ni se cifra la cabecera IP; sin embargo, cuando se utiliza la cabecera de autenticación (AH), las direcciones IP no pueden ser traducidas, ya que eso invalidaría el hash. Las capas de transporte y aplicación están siempre aseguradas por un hash, de forma que no pueden ser modificadas de ninguna manera (por ejemplo, traduciendo los números de puerto TCP y UDP).

    - El modo transporte tiene la ventaja de que asegura la comunicación extemo, pero requiere que ambos extremos entiendan el protocolo IPSec.

  - **Modo Túnel.**

    - En el modo túnel, se cifra o autentica todo el paquete IP (datos más cabeceras del mensaje), es decir, que el contenido del datagrama AH o ESP es un datagrama IP completo, incluida la cabecera IP original.

    - Así, se toma un datagrama IP al cual se añade inicialmente una cabecera AH o ESP, posteriormente se añade una nueva cabecera IP que es la que se utiliza para encaminar los paquetes a través de la red, de otra forma no funcionaría el enrutamiento.

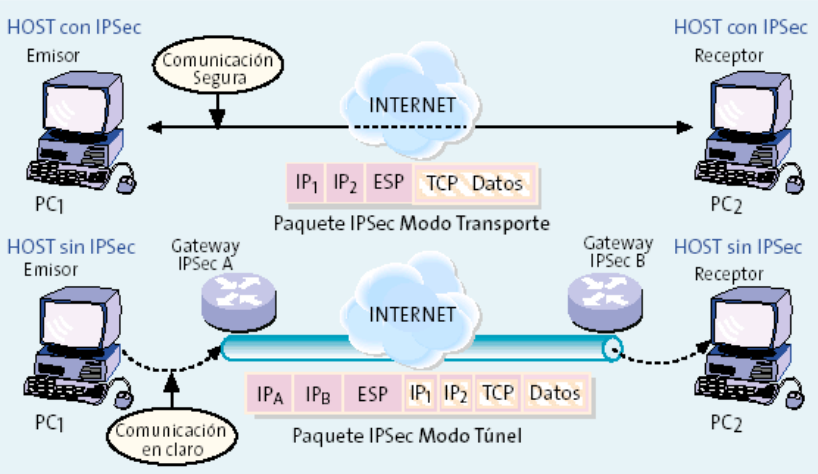
    - Las principales **aplicaciones** del modo túnel son:

      - Cuando el destino final de los datos no coincide con el dispositivo que realiza las funciones IPSec.

      - Para comunicaciones red a red (túneles seguros entre routers) o comunicaciones ordenador a red u ordenador a ordenador sobre Internet.

      - Es empleado principalmente por los gateways IPSec, con objeto de identificar la red que protegen bajo una misma dirección IP y centralizar de este modo el procesado del tráfico IPSec en un equipo.

      - También es útil cuando se utiliza junto con ESP, para ocultar la identidad de los nodos que se están comunicando.



3.3.4 AUTENTICACIÓN EN LA CAPA DE TRANSPORTE: TLS (SSL)

Este protocolo se utiliza en el nivel inferior de ciertas aplicaciones conocidas de Internet, entre las que destacan:

- HTTPS: puerto 443
- SMTPS: puerto 465
- LDAPS: puerto 646
- TELNETS: puerto 992
- IMAPS: puerto 993
- POPS: puerto 995
- FTPS: puertos 989 y 990

- **Transport Layer Security** (TLS; en español «seguridad de la capa de transporte») y su antecesor **Secure Sockets Layer** (SSL; en español «capa de conexión segura») son protocolos criptográficos que proporcionan comunicaciones seguras por una red, comúnmente Internet.

- Se **usan certificados X.509** y por lo tanto **criptografía asimétrica** para autentificar a la contraparte con quien se están comunicando y para intercambiar una llave simétrica.

- TLS es un protocolo **Internet Engineering Task Force** (IETF), definido por primera vez en 1999 y actualizado por última vez en el **RFC 5246** (agosto de 2008) y en **RFC 6176** (marzo 2011). Se basa en las especificaciones previas de SSL (1994, 1995, 1996) desarrolladas por Netscape Communications para agregar el protocolo HTTPS a su navegador Netscape Navigator.

- **Versiones**:

  - **SSL 3.0**: La versión 1.0 nunca se entregó públicamente; la versión 2.0 se presentó en febrero de 1995 pero "contenía una cantidad de fallas de

seguridad que al final llevaron al diseño de la versión SSL 3.0". En el mes de octubre de 2014, se generó una nueva vulnerabilidad sobre el protocolo SSL en su versión 3.0. Ya no se recomienda su uso. “ssl ha muerto”

Algunos ataques:

- En 2011 el ataque BEAST rompe TLS 1.0/SSL 3.0.

- En 2012 ataque CRIME. Vulnerabilidad en algoritmos de compresión que ocasionalmente se usan en TLS 1.0/SSL 3.0. TLS 1.2 no los usa

  SSL ya no es seguro. Tampoco es seguro TLS 1.0

- En 2014 Ataque Poodle:

  ¿Cómo funciona Poodle?

  El ataque POODLE (del inglés "Padding Oracle On Downgraded Legacy Encryption") es un exploit man-in-the-middle que aprovecha Internet y la característica del software de clientes de bajar a SSL 3.0. Si los atacantes explotan exitosamente esta vulnerabilidad, en promedio, solo necesitan hacer 256 solicitudes SSL 3.0 para revelar un byte de los mensajes cifrados. El equipo de Seguridad de Google descubrieron esta vulnerabilidad; la hicieron pública el 14 de octubre de 2014 (a pesar de que el estudio estaba fechado en "Septiembre de 2014"). El ataque POODLE no es tan serio como Heartbleed. El 8 de diciembre de 2014 se anunció una variación al ataque POODLE que impactaba TLS.

  Básicamente consiste en aprovecharse de una característica que hace que, cuando un intento de conexión segura falla, se proceda a intentar realizar de nuevo esa conexión, pero con un protocolo de comunicación más antiguo.

- **TLS 1.0**: es una actualización de SSL versión 3.0. Como dice el RFC, "las diferencias entre este protocolo y SSL 3.0 no son dramáticas, pero son significativas en impedir la interoperabilidad entre TLS 1.0 y SSL 3.0". TLS 1.0 incluye una forma en la cual la implementación puede conectarse en SSL 3.0, debilitando la seguridad.

- **TLS 1.1**: en 2006. Es una actualización de TLS 1.0.

- **TLS 1.2**: en 2008.

- **TLS 1.3** (borrador): Hasta mayo de 2015, TLS 1.3 es un borrador, y los detalles no se han fijado todavía

  Aprobado por el IETF en 2018
  https://www.redeszone.net/2018/03/26/aprobado-estandar-tls-1-3/

Ver cifrado AEAD. AES-GCM
https://www.redeszone.net/2016/12/27/openvpn-2-4-soportara-aead-con-aes-gcm-por-que-esto-es-importante/

Protocolo TLS

- El protocolo consta de **tres fases básicas**:

  - El negociado de algoritmos.
  - El intercambio de claves con autenticación.
  - El cifrado simétrico de los mensajes.

- **Los algoritmos típicos son**:

  - Intercambio de claves: RSA, Diffie Hellman.
  - Autenticación: RSA, DSA (basado en SHA).
  - Cifrado: 3DES, DES, AES, IDEA, RC4.
  - Hash: MD5 y SHA-1.

- Dentro del proceso de comunicación segura **hay dos estados fundamentales:**

  - **Estado de sesión**.

    - Identificador de sesión: número arbitrario elegido por el servidor para identificar la sesión.
    - Certificado x509v3.
    - Método de compresión.
    - Algoritmo de cifrado: algoritmo simétrico para confidencialidad y una función hash para la integridad.
    - Clave maestra: número de 48 bytes secreto entre el servidor y el cliente, y diferente en cada sesión.
    - Flag de nuevas conexiones: indica si desde esta sesión se pueden iniciar nuevas conexiones.

  - **Estado de conexión**.

    - Números aleatorios del servidor y del cliente: números de inicio de la secuencia elegidos por cliente y servidor.
    - Número secreto del cliente para MAC: para calcular los MAC de sus mensajes.
    - Número secreto del servidor para MAC: para calcular los MAC de sus mensajes.
    - Clave secreta del cliente: para cifrar sus mensajes.
    - Clave secreta del servidor: para cifrar sus mensajes.
    - Vectores iniciales: por si se usa cifrado CBC, habrá un vector inicial para cada clave.

- Números de secuencia: cada parte actualiza números de secuencia en cada mensaje y se ponen a cero cuando se recibe un mensaje change cipher spec.

- **TLS se puede considerar dividido en dos capas**.

  - **Protocolo SSL Handshake**.

    - **SubProtocolo ChanceCipherSpec**.

      - SSL actúa como una máquina de estados, con un estado de escritura activo y otro pendiente (tanto para el intercambio de datos como para la lectura) y el cambio de estados se realiza mediante un subprotocolo especial del Handshake denominado subprotocolo Change Cipher Spec.
      - Consta de un simple mensaje con el que se transmite el inicio de cifrado a la otra parte de la comunicación

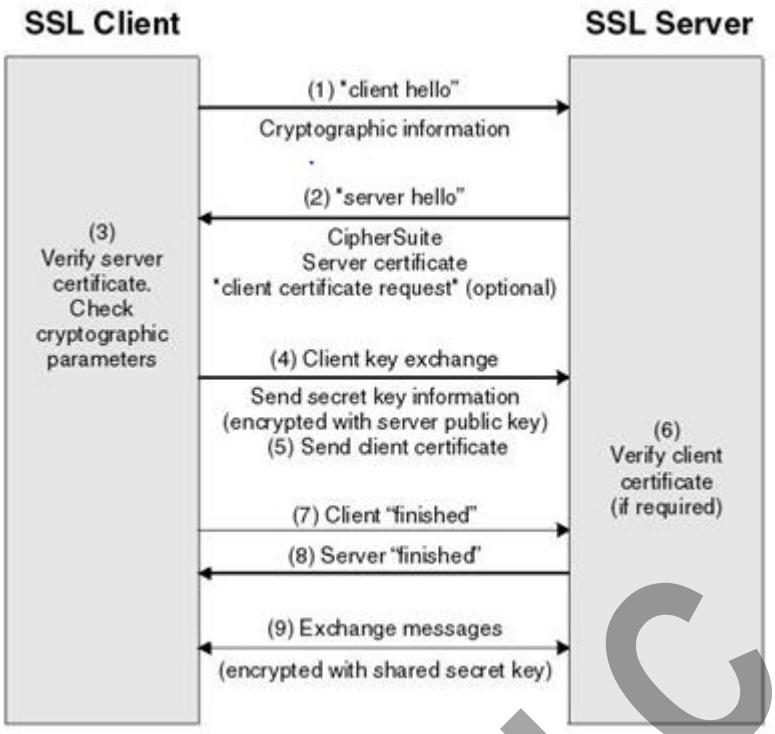
    - **SubProtocolo SSL Alert.**

      - Para avisar de los problemas que ocurren durante la conexión.

  - **Protocolo SSL Record**.

    - Encargado de la seguridad en el intercambio de los datos que llegan desde la capa de aplicación, usando los algoritmos negociados en la fase de Handshaking.

    - Para acordar el formato de datos a usar en la transmisión cifrada, se establecen 3 componentes para la porción de datos del protocolo:
      - MAC-DATA: código de autenticación del mensaje.
      - ACTUAL-DATA: datos de aplicación a transmitir.
      - PADDING-DATA: datos para rellenar el mensaje cuando se usa cifrado en bloque.



Server key Exchange solo se usa cuando no hay certificado

This message will be sent immediately after the server Certificate message (or the ServerHello message, if this is an anonymous negotiation).

The ServerKeyExchange message is sent by the server only when the server Certificate message (if sent) does not contain enough data to allow the client to exchange a premaster secret. This is true for the following key exchange methods:

DHE_DSS
DHE_RSA
DH_anon

It is not legal to send the ServerKeyExchange message for the following key exchange methods:

RSA
DH_DSS
DH_RSA

3.3.5 AUTENTICACIÓN EN SERVICIOS WEB: SAML (SECURITY ASSERTION MARKUP LANGUAGE)

En entornos de acceso a servicios web (Web Services), es necesario ofrecer una especificación que permita que los usuarios puedan visitar múltiples sitios web sin necesidad de identificarse varias veces. Para ello es necesario el intercambio de mensajes XML de autorización y autenticación entre los diferentes servicios de los sitios web.

De esta forma, **OASIS** (*Organization for the Advancement of Structured Information Standards*) desarrolla una especificación de seguridad basada en XML para el intercambio de información de autorización y autenticación que denomina **SAML**. SAML especifica el formato de las sentencias a utilizar y un protocolo de solicitud/respuesta para este intercambio.

SAML intercambia información de autenticación entre el proveedor de servicios y el proveedor de identidad. El proveedor de identidad permite autenticar los usuarios y se pasa la información de identificación a los servicios a modo de un documento XML firmado digitalmente. SAML no autentica ni entiende los procesos de autenticación, sólo es un protocolo para el intercambio de declaraciones de esta autorización.

Estas declaraciones o afirmaciones (aserciones en la nomenclatura SAML) se construyen sobre los atributos y la identidad o sobre las autorizaciones concedidas a entidades autenticadas. Esta información puede ser enviada de forma confidencial aplicando mecanismos criptográficos a los contenidos de estas aserciones.

3.3.6 ACCESO A REDES WIFI

Es importante mencionar los siguientes tres mecanismos de acceso a las redes WiFi:

- **WEP (*Wired Equivalent Privacy*).** Sistema de cifrado para el estándar IEEE 802.11 como protocolo para redes WiFi. Se han descubierto muchas vulnerabilidades del sistema de cifrado WEP, lo que permiten conseguir la clave de conexión en muy poco tiempo. IEEE declaró WEP obsoleto en 2004 y no se recomienda su uso.

- **WPA (*Wi-Fi Protected Access*).** Sistema creado para corregir las deficiencias del anterior, pero se consideraba una opción temporal. Emplea el cifrado con claves dinámicas. En WPA existen varias vulnerabilidades y se desaconseja su uso.

- **WPA-2.** Soluciona problemas de seguridad de la versión anterior y utiliza cifrado simétrico AES. WPA-2 se considera la opción más adecuada, pero tampoco está libre de ataques. Se puede obtener la clave de WPA-2 con ataques de fuerza bruta, aunque debe tenerse en cuenta que el ataque será más complejo según aumenta el tamaño de la clave elegida.

En resumen:

Mecanismo	Cifrado tramas datos	Autenticación	Confianza
WEP	WEP (64 ó 128 bits)	PSK	Nula
WPA	TKIP	PSK ó 802.1x	Media (relativa)
WPA2	CCMP (AES)	PSK ó 802.1x	Alta

Se recomienda encarecidamente para las redes privadas la utilización de WPA-2, si bien no todo el software compatible con WiFi lo soporta. WiMAX (*Worldwide Interoperability for Microwave Access*) utiliza por defecto WPA-2.

Algunas actualizaciones:

Octubre 2017 KRACK Attack, la vulnerabilidad descubierta en WPA2

2018:

WiFi 6 en lugar de WiFi 802.11ax.

Wifi 6 ya es compatible **con los dispositivos actuales, pero todavía no está disponible en el mercado.**

WiFi 6 proporcionará la **capacidad, cobertura y rendimiento requeridos por los usuarios en la actualidad, incluso en entornos densos** como estadios deportivos y otros lugares públicos concurridos. Además, puede presumir de contar con una **eficiencia energética mejorada**

Algunas empresas ya han comenzado a desarrollar chips, aunque la adopción de esta tecnología a nivel a nivel general no se espera hasta 2019

Nuevas nomenclaturas:

- 802.11b se llamará Wi-Fi 1 (no confirmado)
- 802.11a se llamará Wi-Fi 2 (no confirmado)
- 802.11g se llamará Wi-Fi 3 (no confirmado)
- **802.11n se llamará Wi-Fi 4**
- **802.11ac se llamará Wi-Fi 5**
- **802.11ax se llamará Wi-Fi 6**

3.3.7 ACCESO A REDES DE TELEFONÍA MÓVIL

El acceso a este tipo de redes depende del estándar de telefonía móvil. Citar que para el sistema de segunda generación (2G) GSM en las que las comunicaciones se producen de forma digital, se utiliza un método de autenticación EAP denominado EAP-SIM (*EAP for Suscriber Identity Module*) con mecanismos de cifrado (A1 y A5) fácilmente atacables en la actualidad.

La extensión a 3G se denomina UMTS (*Universal Mobile Telecommunications System*) y utiliza autenticación mutua de usuario y de red, mediante un protocolo denominado EAP-AKA (*EAP for UMTS Authentication and Key Agreement*).

La cuarta generación (4G) de tecnología de telefonía móvil está basada completamente en el protocolo IP y está siendo desarrollada para ofrecer un alto nivel de seguridad de este protocolo.

El Centro Criptológico Nacional (CCN) ha publicado varias guías de seguridad para dispositivos móviles. Por ejemplo, en agosto de 2014 se publicaron las guías CCN-STIC 454 y 455 con las recomendaciones de seguridad en móviles basados en el sistema operativo iOS (iPhone e iPad).

3.3.8 CONTROL DE ACCESO A LA RED BASADO EN PUERTOS

Fuente Wikipedia: La IEEE 802.1X es una norma del IEEE para el control de acceso a red basada en puertos. Es parte del grupo de protocolos IEEE 802 (IEEE 802.1). Permite la autenticación de dispositivos conectados a un puerto LAN, estableciendo una conexión punto a punto o previniendo el acceso por ese puerto si la autenticación falla. Es utilizado en algunos puntos de acceso inalámbricos cerrados y se basa en el protocolo de autenticación extensible (EAP– RFC 2284). El RFC 2284 ha sido declarado obsoleto en favor del RFC 3748.

802.1X está disponible en ciertos conmutadores de red y puede configurarse para autenticar nodos que están equipados con software suplicante. Esto elimina el acceso no autorizado a la red al nivel de la capa de enlace de datos.

Algunos proveedores están implementando 802.1X en puntos de acceso inalámbricos que pueden utilizarse en ciertas situaciones en las cuales el punto de acceso necesita operarse como un punto de acceso cerrado, corrigiendo deficiencias de seguridad de

WEP. Esta autenticación es realizada normalmente por un tercero, tal como un servidor de RADIUS. Esto permite la autenticación sólo del cliente o, más apropiadamente, una autenticación mutua fuerte utilizando protocolos como EAP-TLS.

No confundir con NAC: Control de acceso a red (del inglés Network Access Control, NAC) es un enfoque de la seguridad en redes de computadoras que intenta unificar la tecnología de seguridad en los equipos finales (tales como antivirus, prevención de intrusión en hosts, informes de vulnerabilidades), usuario o sistema de autenticación y reforzar la seguridad de la red de acceso.

4 TÉCNICAS CRIPTOGRÁFICAS

Estas técnicas se estudian en el tema de cifrado. Algoritmos de cifrado simétricos y asimétricos. La función hash. El notariado.

5 CONTROL DE INTRUSIONES

5.1 SISTEMA DE DETECCIÓN DE INTRUSIONES: IDS (INTRUSION DETECTION SYSTEM)

Los IDS monitorizan los eventos de la red y sus sistemas cuya función es detectar posibles intrusiones y accesos no autorizados. Estos sistemas tienen sensores internos a la red, con los cuales capturan el tráfico y lo analizan intentando encontrar patrones de ataques conocidos (a semejanza de lo que haría un analista humano, pero a una velocidad infinitamente mayor). La base de datos de ataques, análogamente a los antivirus, suele llamarse base de datos de "firmas". Existen dos tipos de IDS, en función del lugar en que se instalen:

- **Network intrusion detection system** (NIDS): Conectado a un segmento de red. Trabaja sobre un puerto espejo o *mirror* al que se vuelca todo el tráfico que pasa por los conmutadores de red de nivel dos, o *switches*.

- **Host-based intrusion detection system** (HIDS): IDS software que analiza todos los *logs* de un equipo. El IDS reside generalmente dentro del propio equipo monitorizado.

Los IDS pueden asumir acciones de respuesta ante intrusiones y ser más activos, pero lo habitual es separar esta función en los sistemas de prevención de intrusión IPS.

Los IDS para su funcionamiento capturan el tráfico que pasa por un switch a través de un puerto espejo o port mirroring. También se conocen como puerto SPAN (Switched Port Analyzer)

SAT (Sistema de Alerta Temprana) de CCN-CERT son IDS
Existen dos: SAT-INET que se ubica en la zona perimetral de Internet y SAT-SARA ubicado en la conexión con la Red SARA
SAT estaban basados en SNORT y actualmente se basan en SURICATA

Más información: https://www.ccn-cert.cni.es/gestion-de-incidentes/sistema-de-alerta-temprana-sat.html

5.2 SISTEMA DE PREVENCIÓN DE INTRUSIONES: IPS (INTRUSION PREVENTION SYSTEM)

Los IPS intentan actuar en la red para eliminar las amenazas que detectan, siempre en función de las políticas que rigen su configuración. Los IPS protegen al equipo

proactivamente y bloquean los ataques y, por esta razón, generalmente suelen estar acompañados de un software de firewall asociado o trabajar de forma combinada con el cortafuegos.

El despliegue de los sistemas IPS, dentro de una red, es diferente a los IDS y se sitúan de forma diferente. Como se ha comentado, los IDS se colocan en puertos de los *switches* donde se vuelca toda la información de la red de forma replicada, mientras que los IPS se ubican en los enlaces más importantes, de forma que el tráfico se curse a través de ellos, y puedan así ser más efectivos a la hora de eliminar tráfico malicioso. Cuando se colocan los IPS, al poder convertirse en un único punto de fallo de toda la red, se debe asegurar que la red continúe operando en esa eventualidad. De esta forma, los IPS vienen equipados con técnicas de redundancia y se suelen configurar en alta disponibilidad. Estos *appliances* actualmente están teniendo gran éxito en el mercado.

Fabricantes: Checkpoint, Dell SonicWall, Fortinet FortiGate, HP TippingPoint, McAfee NS, Cisco Sourcefire, McAfee Stonesoft

5.3 WIPS. WIRELESS IPS

- Defienden de Puntos de acceso no autorizados en la red. Los clasifican en:
    - Autorizados
    - Externos (puntos de accesos cercanos, pero no conectados a nuestra red)
    - No autorizados (puntos de acceso desconocidos que se conectan a nuestra red, el WIPS bloquea las conexiones de los usuarios a ese punto de acceso)
- Previenen de puntos de acceso que simulan ser nuestros puntos de acceso bloqueando a los usuarios su conexión a estos puntos de acceso
- Suprime ataques de denegación de servicio. Los clientes maliciosos pueden utilizar paquetes de desautenticación para intencionalmente bloquear conexiones a su red. El WIPS suprime estos ataques de negación de servicio mediante la búsqueda continua de grandes cantidades de paquetes de desautenticación en el aire. Luego, se identifica la fuente y se bloquea todos los tipos de transmisión adicionales.

5.4 LOS GESTORES DE EVENTOS (ANÁLISIS DE LOGS)

En las grandes redes donde los IDS de red no tienen suficiente información para poder detectar ataques, es necesaria una gestión centralizada de todos los eventos relacionados con patrones sospechosos y una monitorización de la infraestructura. Asimismo, debe existir una correlación

de eventos y una visibilidad conjunta de los diferentes sistemas de seguridad (cortafuegos, IDS, IPS, etc).

El análisis y la gestión de logs y la correlación de eventos (SIEM - *Security Information and Event Management*) es un parte importante de la gestión de riesgos de seguridad de la información. SIEM describe las capacidades de los productos de recopilación, análisis y presentación de información de la red y los dispositivos de seguridad, las aplicaciones de gestión de identidades y accesos, gestión de vulnerabilidades y los instrumentos de política de cumplimiento, sistema operativo, base de datos y registros de aplicaciones.

Fabricantes: HP ArcSight, EMC RSA; AlienVault, OSSIM, Splunk, SolarWinds, IBM Qradar, Lógica.

NOTA: GLORIA es un sistema SIEM DEL CCN-CERT

6 CORTAFUEGOS (FIREWALLS)

6.1 TEORÍA DE CORTAFUEGOS. TIPOS DE POLÍTICAS.

Los cortafuegos, en el ámbito de las redes de comunicaciones, se corresponden con programas o dispositivos de red que se encargan de permitir, denegar, cifrar, descifrar, modificar o cachear el tráfico de una red empleando políticas que definen un conjunto de criterios y normas.

Los cortafuegos analizan los paquetes y en función del nivel del análisis, y las políticas según las que estén configurados, efectuarán determinadas acciones sobre el tráfico. El modo de funcionamiento típico de un *firewall* es el siguiente:

- Recibir todo el tráfico entrante por las interfaces de red monitorizadas.
- Comprobar si el tráfico se corresponde con alguno de los patrones marcados en las políticas definidas en el *firewall*. Las políticas están ordenadas por prioridades, y se comienza por comparar el tráfico desde la de mayor prioridad hasta la de menos.
- Si el tráfico cumple los patrones de alguna política (como por ejemplo "*puerto TCP de destino 53*") entonces se aplica la acción predefinida en la regla correspondiente (por ejemplo "*DENY*").
- Si el tráfico no cumple ninguna regla del firewall, se aplicará la regla por defecto. Para definirla, siempre, en la última regla de prioridad se configura una de estas dos políticas: "*ACCEPT ALL"* o "*DENY ALL"*, que constituyen las políticas por defecto. En general, es altamente recomendable dejar como política por defecto "*DENY ALL*", sobre todo si el firewall está expuesto a Internet. Para las LAN corporativas, depende de las decisiones de los administradores de red.

Hay dos políticas básicas en la configuración de un cortafuegos y que cambian radicalmente la filosofía fundamental de la seguridad en la organización:

- **Política restrictiva**: Se deniega todo el tráfico excepto el que está explícitamente permitido. El cortafuegos obstruye todo el tráfico y hay que habilitar expresamente el tráfico de los servicios que se necesiten (es el caso del "*DENY ALL"* como política por defecto).

- **Política permisiva**: Se permite todo el tráfico excepto el que esté explícitamente denegado. Cada servicio potencialmente peligroso necesitará ser aislado básicamente caso por caso, mientras que el resto del tráfico no será filtrado ("*ACCEPT ALL"* como política por defecto).

La política restrictiva es la más segura, ya que es más difícil permitir por error tráfico potencialmente peligroso y es la que debe utilizarse en empresas y organismos.

Las diferentes tecnologías de cortafuegos se diferencian por el nivel de red en el que se realizan las inspecciones, el estado de las conexiones y las operaciones que pueden realizar con el tráfico. A continuación, se muestras las tecnologías comúnmente usadas.

National Institute of Standards and Technology (NIST) ha publicado la Special Publication 800-41 con, con una serie de directivas y consejos para ayudar a los administradores de seguridad en la implementación de los sistemas de filtrado perimetral

6.2 TECNOLOGÍAS DE CORTAFUEGOS

6.2.1 CORTAFUEGOS DE RED (PACKET FILTERING)

Estos cortafuegos operan a nivel de red en la pila TCP/IP. Consiste en filtrar paquetes de red con la información de cabeceras IP y TCP. El filtrado se basa en las direcciones origen y destino, el protocolo, los puertos origen y destino, el tipo de mensaje y los interfaces de entrada y salida de la trama en el router.

En este grupo de cortafuegos existen dos clasificaciones:

- ***Filtrado de paquetes dinámico (Stateful packet filtering)***: Estos firewalls guardan información de las sesiones a las que pertenecen los paquetes, y si vuelven a aparecer paquetes que pertenecen a una sesión aceptada, se acepta con mayor rapidez. Estos firewalls, si bien requieren más memoria, son mucho más rápidos que los siguientes.

- ***Filtrado de paquetes estático (Stateless packet filtering)***: son cortafuegos que analizan cada paquete independientemente de las posibles sesiones abiertas con anterioridad.

6.2.2 CORTAFUEGOS A NIVEL DE APLICACIÓN (APPLICATION FIREWALL)

Estos cortafuegos funcionan por encima del nivel TCP, analizando los protocolos específicos de las aplicaciones que utilizan TCP. Analizan por ejemplo el protocolo HTTP, FTP, SMTP…. Este tipo de cortafuegos realiza una auditoría y registro del tráfico que pasa a través del dispositivo y los filtros se realizan a nivel de aplicación, por lo que permite el filtrado del protocolo. Además, adicionalmente este tipo de cortafuegos suelen prestar servicios de autenticación de usuarios, dado que están en la capa de aplicación.

Su funcionamiento consiste en reconstruir los paquetes a ese nivel de aplicación, por lo que requieren elevada memoria y capacidad de procesamiento. Comprueban que las peticiones se adecúen a las políticas especificadas (por ejemplo, no descargar mediante *ftp* ningún archivo "*.exe*", o realizar escaneo de antivirus de los archivos descargados). Al funcionar a nivel de aplicación, deben reconstruir las tramas para poder analizar la petición completa.

Principales WAF (Web App Firewall) Hardware: Barracuda, CITRIX Netscaler, F5 Big-IP, Fortinet Fortiweb, Imperva SecureSphere

WAF Software muy utilizado: mod_security de Apache desarrollado por Breach Security.

"As today's web application attacks expand and their relative level of sophistication increases, it is vitally important to develop a standardized criteria for WAFs evaluation. The Web Application Firewall Evaluation Criteria Project (WAFEC) serves two goals:

- *Help stakeholders understand what a WAF is and its role in protecting web sites.*
- *Provide a tool for users to make an educated decision when selecting a WAF."*

Hoy en día cualquier dispositivo de este tipo engloba múltiples funcionalidades en la misma máquina. Son conocidos como **UTM** (Unified Threat Management) o Gestión Unificada de Amenazas

- UDP
- VPN
- Antispam
- Antiphishing
- Antispyware
- Filtro de contenidos

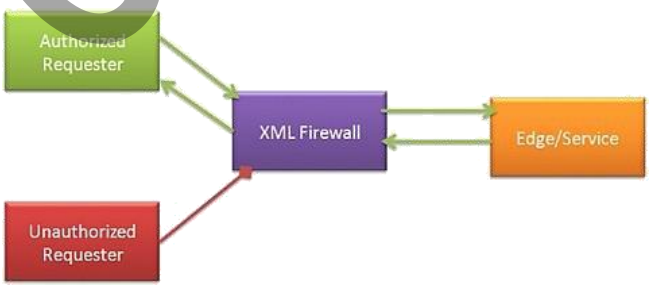
- Antivirus
- Detección/Prevención de Intrusos (IDS/IPS)

Se trata de cortafuegos a nivel de capa de aplicación que pueden trabajar de dos modos:

- Modo proxy: hacen uso de proxies para procesar y redirigir todo el tráfico interno.
- Modo Transparente: no redirigen ningún paquete que pase por la línea, simplemente lo procesan y son capaces de analizar en tiempo real los paquetes. Este modo, como es de suponer, requiere de unas altas prestaciones de hardware.

Se debe destacar dentro de estos cortafuegos a los *proxys*. El *proxy* controla el tráfico de un determinado protocolo (como HTTP) y permite controlar los sitios web a los que los usuarios se conectan, así como llevar un registro de las conexiones. Este tipo de cortafuegos permite servicios avanzados de políticas, como filtrar las webs de contenido malicioso actualizando las listas desde Internet.

Un proxy interesante es el que realiza análisis de mensajes XML en el protocolo de transporte HTTP. Los *firewalls* XML se encargan de analizar todas las peticiones XML realizando labores de filtrado XML con verificación de paquetes y validación de esquema. Este tipo de cortafuegos está especialmente indicado para los servicios web, y cumplen las especificaciones de WS-Security para la supervisión del tráfico. Estos dispositivos también se conocen como *XML Security Gateways*. El siguiente croquis recoge el funcionamiento básico de un cortafuegos XML:



Las funcionalidades y beneficios de los *Firewall XML*:

- Verificación de paquetes. Mensajes bien formados.
- Validación del esquema XML. Mensajes que cumplen el esquema XML esperado.

- Validación de datos. Aceptación o rechazo de tráfico XML entrante/saliente.
- Control de acceso. Autenticación y autorización de los accesos.
- Gestión de ficheros adjuntos con integración con antivirus.
- Protección frente ataques.

6.2.3 SERVICIOS ADICIONALES DE LOS CORTAFUEGOS

La tecnología de cortafuegos además de permitir el filtrado de paquetes y de aplicaciones, suelen añadir algunas funcionalidades típicas que facilitan las labores de protección y administración de la red:

- Translación de Direcciones de Red (**NAT -** *Network Address Translation*): permite la modificación "al vuelo" de paquetes IP y de los puertos TCP, para enmascarar puertos y direcciones IP. De esta forma, se consigue esconder las direcciones de red reales de la red interna.

- Redes privadas virtuales (**VPN** – *Virtual Private Network*): al estar conectados en los perímetros de las redes, suelen acompañar la posibilidad de crear conexiones VPN tipo túnel para acceder a la red de la organización. El equipo que crea los túneles VPN no se coloca detrás del cortafuegos, ya que en ese caso el tráfico cifrado entrante y saliente generado por el servidor VPN no podría ser inspeccionado.

Tipos de VPN: (Pregunta examen A1 2017)

- **VPN de acceso remoto:** Los usuarios que se conectan con la empresa desde sitios remotos (oficinas comerciales, domicilios, hoteles, aviones preparados, etcétera) utilizando Internet como vínculo de acceso (VPN-PPTP)

- **VPN punto a punto o sitio a sitio.** Este esquema se utiliza para conectar oficinas remotas con la sede central de la organización. El servidor VPN, que posee un vínculo permanente a Internet, acepta las conexiones vía Internet provenientes de los sitios y establece el túnel VPN. Los servidores de las sucursales se conectan a Internet utilizando los servicios de su proveedor local de Internet, típicamente mediante conexiones de banda ancha. Esto permite eliminar los costosos vínculos punto a punto tradicionales (realizados comúnmente mediante conexiones de cable físicas entre los nodos), sobre todo en las comunicaciones internacionales. Es más común el siguiente punto, también llamado tecnología de túnel o tunneling.

- **VPN L2TP** (Layer to Tunneling Protocol)**.** Fue desarrollado por Microsoft y Cisco. Similar a PPTP. Ambas dependen de protocolos PPP.

- **IPSEC** (visto anteriormente)

- **SSL y TLS.** Una herramienta de software libre para estas conexiones es **OpenVPN**

- **VPN MPLS:** Las VPN de conmutación por etiquetas multi-protocolo o MPLS. Dificiles de configurar, más costosas.

- **VPN Híbrida:** Una VPN híbrida combina MPLS y VPN basada en protocolo de seguridad de internet o IPsec, aunque estos dos tipos de VPN se usan por separado en diferentes sitios. Sin embargo, es posible usar ambas en el mismo sitio. Esto se haría con la intención de utilizar la VPN IPsec como un respaldo de la VPN MPLS

- Integración con IDS e IPS: por su especial ubicación en las redes, estos dispositivos son idóneos para realizar las funciones de IDS e IPS ya que todo el tráfico debe pasar por ellos.

7. OTROS DISPOSITIVOS DE SEGURIDAD PERIMETRAL

Terminador VPN con las siguientes funcionalidades:

- Conexión segura de usuarios remotos que accedan desde Internet con dispositivos fijos o móviles.
- Servicio de terminación de túneles VPN.
- Soporte de VPN-SSL, IPSec y ActiveSync (para Microsoft)
- Control de seguridad o chequeo de políticas de dispositivo final (antivirus actualizado, equipo parcheado, etc.)
- Acceso y autenticación con certificados, etc.
- Acceso con y sin cliente o cliente ligero (navegador web)
- Soporte de plataformas de cliente: Windows, Mac, Linux, iOS, Android, Windows Phone, etc
- Posibilidad de autenticación mediante doble factor.

Firewall de Nueva Generación con las siguientes funcionalidades:

- Inspección de tráfico de red y de aplicación.
- Funciones de firewall estándar de primera generación: filtrado de paquetes, traducción de dirección de red (NAT), inspección de protocolo con estado (stateful), capacidades VPN etc.
- IPS integrado con soporte de firmas de vulnerabilidades y amenazas.
- Capacidad de monitorización hasta el nivel Aplicación. Ejemplo: permitir chat de gtalk pero no intercambio de ficheros por el chat.
- Inteligencia: obtener información de fuentes fuera del firewall para tomar decisiones de bloqueo optimizadas.
- Actualización para obtener información de nuevas técnicas que hagan frente a las amenazas futuras.
- Capacidad de inspección de tráfico SSL. Integración con HSMs para el almacenamiento seguro de certificados.
- Capacidades WAF. (esto podría sacarse del FW y ser un dispositivo independiente)

Sistema de control de navegación con las siguientes funcionalidades:

- Antivirus. Detección y eliminación de virus mediante firmas o heurísticas sobre el tráfico de navegación.
- Antimalware, detección y eliminación de programas dañinos mediante firmas o heurísticas sobre el tráfico de navegación.
- Filtro de URLs.
- Filtro de aplicaciones.
- Anti-botnet. Detección de comportamientos anómalos o consulta de una base de datos con URLs o IPs participantes en una red de bots
- Proxy
- Funciones DLP para prevenir fugas de información

Sistema de protección de correo con las siguientes funcionalidades:

- Filtrado para correo entrante y saliente incluyendo filtrado de conexión, antivirus, antispam y antimalware y filtrado de contenidos.
- Funciones de relay de correo para reintentar el envío del correo en caso de caída de los servidores internos de correo.
- Doble motor de antivirus de distintos fabricantes, de reconocida reputación.
- Capacidad para analizar tanto el cuerpo de los mensajes como los adjuntos (incluyendo los archivos adjuntos comprimidos).
- Análisis basado en el tipo de fichero independientemente de su extensión.
- Análisis basado en firmas, análisis heurístico y análisis de imágenes
- Funciones de cuarentena.
- Motor de reglas para correo entrante y saliente.
- Listas de reputación (RBLs),
- Soporte para protocolos de securización de correo como, SPF, greylisting
- filtrado antispoofing.
- Posibilidad de cifrado de correos.
- Configuración de listas blancas y negras
- Funciones DLP para prevenir fugas de información

Sistema de detección de intrusos (IDS) como la sonda SAT INET del CCN

https://www.ccn-cert.cni.es/gestion-de-incidentes/sistema-de-alerta-temprana-sat/sat-inet.html

Sistema de protección AntiDDoS con las siguientes funcionalidades:

- Detección y mitigación de ataques DDoS.
- Mitigación de ataques maliciosos de tráfico y entrega el tráfico limpio.
- Protección contra ataques DDoS volumétricos y orientados a la aplicación.
- Módulo de informes.

Sistema de gestión de ancho de banda con las siguientes funcionalidades:

- Control de conexiones.
- Asignación de ancho de banda por conexión.
- Control de aplicaciones.
- Gestión de ancho de banda y QoS.
- Control P2P.
- Sistema de alertas.
- Módulo central de informes.

Sistema de correlación de eventos con capacidad de recolección, capacidad de detección y capacidad de repuesta.

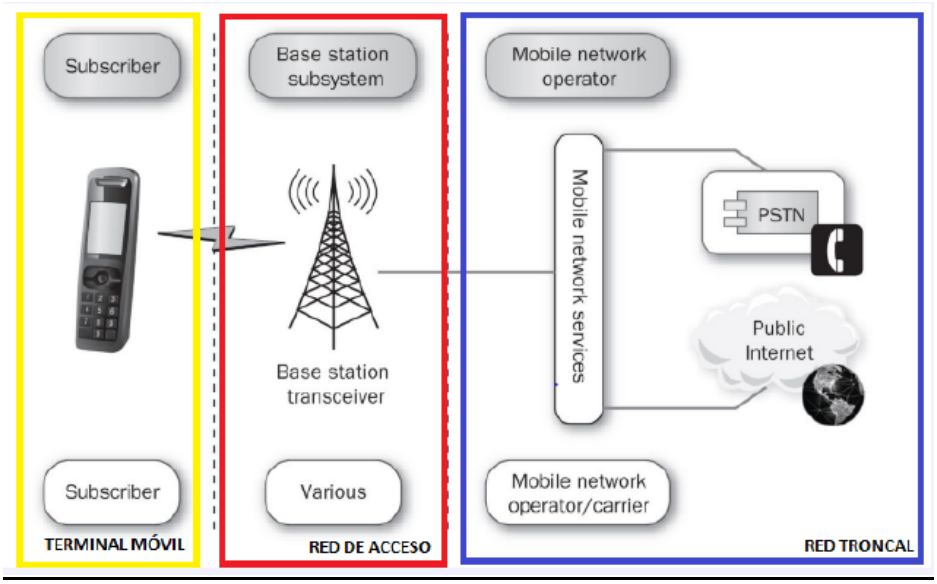
8. SEGURIDAD EN COMUNICACIONES MÓVILES

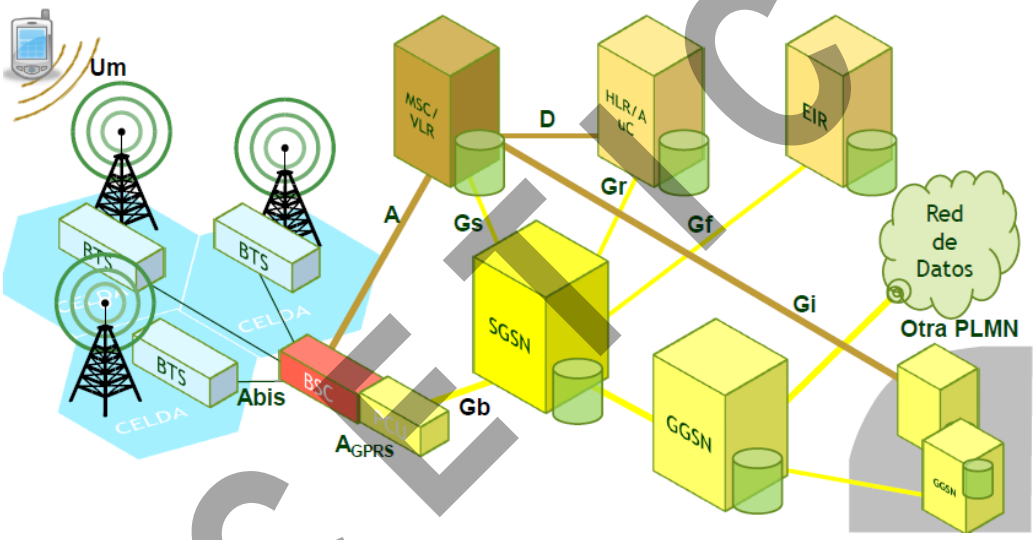
A complementar con el tema de comunicaciones móviles

Terminología

- **SIM** (Subscriber Identity Module) Tarjeta inteligente que contiene el IMSI y la Ki del usuario
- **IMSI** (International Mobile Subscriber Identity) Identificador del usuario
  Estructura:
    - MCC-Mobile Country Code (3 dígitos)
    - MNC- Mobile Network Code (2 dígitos Eu, 3 USA)
    - MSIN- Mobile Station Identification Number (8 o 9)
- **IMEI** Identificador del terminal (teléfono / modem)
  Estructura:
    - TAC-Type Allocation Code (2+6=8 dígitos)
    - Serial Number (6dígitos)
    - Checksum (1 dígito)
- **Ki** Clave precompartida entre la tarjeta SIM y el operador
- **Kc** Clave de sesión (generada dinámicamente en cada sesión)
- **BTS/nodeB/e-nodeB Estación base**. Llamada coloquialmente: "antena del operador"
- **SGSN, GGSN** Nodos de la red del operador que cursan el tráfico IP, el GGSN es la puerta de enlace con la red Exterior
- **PLMN** Red de un operador (Public Land Mobile Network)
- **MSC** central de conmutación móvil. Centralita telefónica para la conmutación de llamadas
- **HLR** *(Home Location Register,* o **registro de ubicación base)** es una base de datos que almacena la posición del usuario dentro de la red, si está conectado o no y las características de su abono (servicios que puede y no puede usar, tipo de terminal, etcétera). Es de carácter más bien permanente; cada número de teléfono móvil está adscrito a un HLR determinado y único, que administra su operador móvil.
- **MS** Mobile station. Estación móvil

Arquitectura





Tecnología móvil

1G: Primeros estándares de "telefonía Móvil"

En un principio no había estándar, por lo que la telefonía de primera generación (1G) solía cubrir únicamente el país donde se había desarrollado, al ser incompatible con las redes del resto de países. En esta generación, la tecnología era toda analógica, a excepción de la señalización (geoposicionamiento entre satélite y teléfono), que era digital.

La voz viajaba en claro, simplemente modulada en frecuencia.

8.1 SEGURIDAD EN COMUNICACIONES GSM

Algunos datos:

- Sistema celular digital
- Modulación GMSK
- Conmutación de circuitos
- Canales de voz a 13 Kbps
- Mínimas capacidades de datos:
- 9,6 kbps por circuito de datos (CSD)

Proceso de autenticación:

Se trata de un mecanismo de desafío respuesta

El suscriptor se identifica únicamente con un código único, llamado IMSI (International Mobile Subscriber Identity), guardado en la SIM.

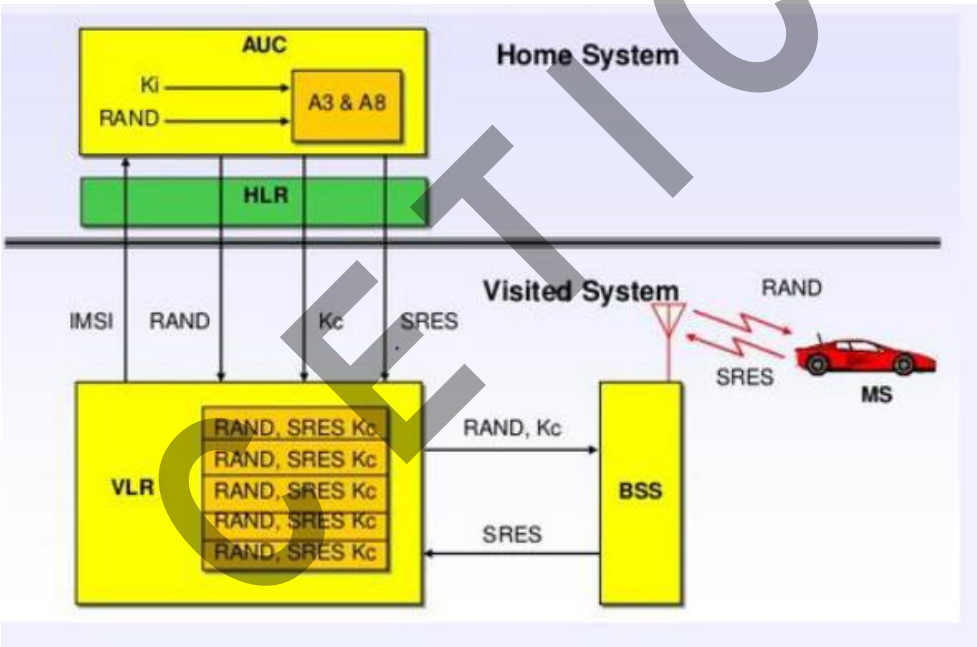
Esta clave está también en el AuC asociado al HLR al que pertenece el móvil.

En la SIM también están la clave única de usuario (Ki), el algoritmo de generación de claves de cifrado (A8), el algoritmo de autenticación (A3) y el PIN. En el móvil GSM está el algoritmo de cifrado (A5).

Cuando se inicia el proceso de autenticación, se informa de esto al VLR visitado y comienza el proceso bajo su control. La red GSM le pide al móvil su IMSI, y lo comunica al HLR. El HLR envía el IMSI al AuC, que dispone de una tabla con la relación IMSI<->Ki

de todos sus abonados (esta tabla puede estar implementada en una base de datos distribuida cuando el número de abonados de la red es demasiado grande). Con la clave Ki y un número aleatorio, se utiliza un algoritmo tipo A3 para calcular una respuesta firmada, que es enviada al VLR visitado por el móvil. También se utiliza un algoritmo tipo A8 para conseguir una nueva clave Kc a partir de Ki y el número aleatorio. Esta clave Kc se utiliza para el cifrado de la información en el canal de tráfico.

El número aleatorio se envía al móvil para que éste, realice el mismo proceso (utilizando los mismos algoritmos) y calcule Kc y la respuesta firmada. La respuesta firmada se envía al VLR visitado, y éste comprueba que coincide con lo calculado por el AuC de la red. Si es así, el proceso de autenticación ha sido positivo.
Ki y RAND son de 128 bits
Kc 64 bits
SRES 32 bits

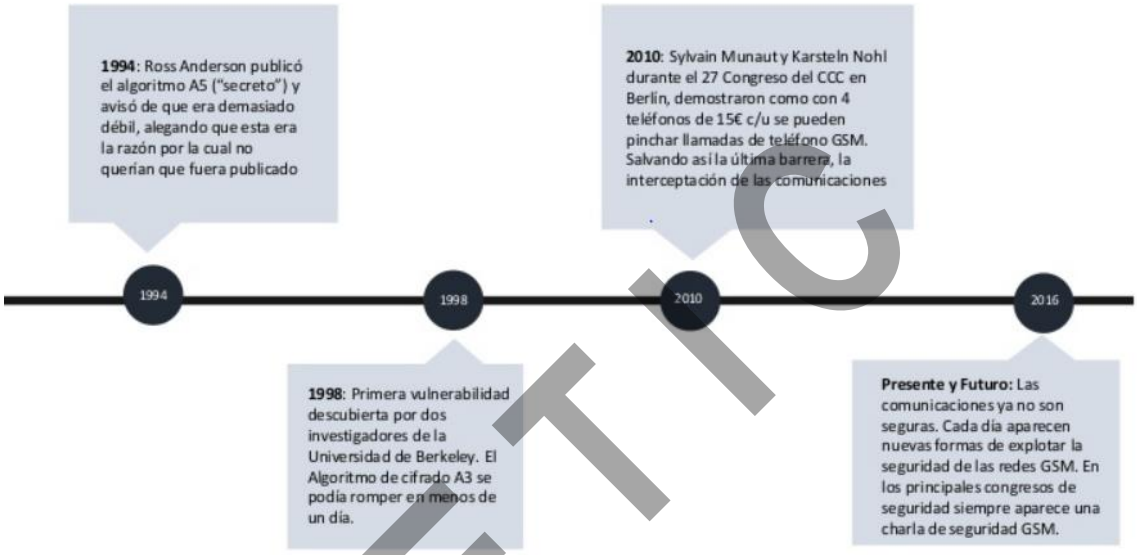


Cifrado

GSM cifra, a partir de un momento en la comunicación, la voz y los datos de señalización.
Normalmente el cifrado se realiza con el algoritmo A5/1
El algoritmo A5/1 es un algoritmo que genera un bitstream por cada unidad de transmisión (ráfaga).
El bitstream se combina (XOR) con la ráfaga a transmitir
La generación del bitstream depende de una clave de sesión y del número de trama TDMA.

Vulnerabilidades de GSM

- IMSI revela la ubicación de un usuario
- La norma sugiere el uso de A5/0 como método de cifrado.
- Debilidades de los algoritmos de cifrado.
- **MS no autentica la red (infiltración en red del operador)**
- La obtención de Kc solo depende de RAND y Ki
- El protocolo SS7 es vulnerable. Este protocolo es utilizado principalmente para el establecimiento y finalización de llamadas, aunque también tiene otros usos El SS7 se estandarizó en los años ochenta.



8.2 SEGURIDAD EN COMUNICACIONES GPRS

Autenticación:

El procedimiento de autentificación de usuario en GPRS es similar al utilizado en GSM. La diferencia es que el procedimiento es ejecutado desde el SGSN en lugar que desde MSC.

El mecanismo de autentificación utiliza tripletas de identificación que se reciben del HLR y se almacenan en el SGSN. Las tripletas de identificación consisten en:

- RAND: un número aleatorio entre 0 y 2^{128}-1.
- SRES: respuesta con firma que es el resultado del algoritmo de cifrado A3 utilizado para la autentificación del subscriptor.
- Kc: es la clave de cifrado calculada usando el algoritmo A8 y que es usado por el algoritmo de cifrado GPR, GEA (GPRS Encryption Algorithm).

El algoritmo A3 utilizado para calcular SRES depende del operador, mientras permita la técnica de *roaming* a través de la red pública terrestre de móviles, PLMN (Public Land

Mobile Network). Los operadores pueden elegir un algoritmo A3 aplicable a sus propios subscriptores. Sin embargo, el ETSI ha diseñado un algoritmo, y los operadores pueden utilizarlo si quieren. El algoritmo A3 del ETSI es secreto.

Es importante anotar que todas las funciones de seguridad dentro de la red GPRS están basadas en la clave secreta Ki. Esta es almacenada en la tarjeta módulo de identificación de usuario, SIM (Subscriber Identification Module) y en el HLR

Durante el proceso de autentificación el SGSN informa a la MS si se utiliza algoritmo de cifrado o no.

Cifrado

El cifrado se realiza entre el SGSN y la estación móvil

En GRPS los datos y la señalización son cifrados durante la transferencia. La funcionalidad de cifrado está situada en la capa LLC. El método de cifrado es el algoritmo de encriptación GPRS, GEA (GPRS Encryption Algorithm), que es secreto. El rango de cifrado en GRPS es desde la función de cifrado en SGSN a la función de cifrado en la MS en contraste con el cifrado GSM, con un solo canal lógico entre BTE y MS.

Algoritmos obligatoriamente soportados por una MS (estación móvil) GPRS:

- GEA0 = NO cifrado
- GEA1 = Roto mediante algebraic attacks (*)
- GEA2 (utilizado comúnmente)
- GEA3

GPRS soporta QoS

Comparativa con GSM

8.3 SEGURIDAD EN COMUNICACIONES 3G

El **3GPP** (3rd Generation Partnership Project: Proyecto Asociación de Tercera Generación) es una colaboración de grupos de asociaciones de telecomunicaciones, conocidos como miembros organizativos. El objetivo inicial del 3GPP era asentar las especificaciones de un sistema global de comunicaciones de tercera generación 3G para teléfonos móviles basándose en las especificaciones del sistema evolucionado GSM. ETSI es miembro organizativo del 3GPP en Europa.

Algoritmos obligatoriamente soportados por una MS UMTS:

- UEA0 = NO cifrado
- UEA1 = KASUMI (también A5/3)
- Probablemente roto por la NSA para claves de 64 bits.
- UEA2 = SNOW-3G

- Autenticación bidireccional
- Confidencialidad de las comunicaciones
- Integridad de las comunicaciones
- Confidencialidad de la identidad del usuario

Vulnerabilidades potenciales:

- IMSI cátcher

Una de las principales ventajas del 3G es que la red debe identificarse frente al móvil, y no solo a la inversa, como ocurría en 2G. La red será legítima si conoce una clave secreta almacenada en el terminal, que viaja cifrada. Hay una forma de esquivar esta barrera. El protocolo de las comunicaciones 3G permite cierto intercambio de información entre la red y el dispositivo antes de que se produzca esta autenticación y entre en juego la criptografía.

- Localización geográfica

Gracias al código IMSI que se podría capturar en el primer ataque, se puede establecer un canal de radio con el móvil (un móvil concreto, que se sabe a quién pertenece) y mantenerlo abierto el tiempo suficiente para que dé tiempo a triangular su posición y mostrarla en una pantalla.

- Denegación de servicio

Antes de que se produzca la autenticación y el intercambio comience a estar cifrado, la falsa red que suplanta a la operadora envía un código de rechazo al dispositivo móvil,

denegándole la conexión. Así, **el teléfono se queda sin cobertura 3G y no la recupera** hasta que se produzca un reinicio.

- 'Downgrade' selectivo

Este ataque, exclusivo de 3G, es algo así como la llave maestra de todos los ataques, puesto que **obliga al móvil a conectarse a la antigua e insegura red 2G**.

8.4 SEGURIDAD EN COMUNICACIONES 4G

Algoritmos obligatoriamente soportados por una MS LTE:

- EEA0 = NO cifrado
- 128-EEA1 = SNOW-3G
- 128-EEA2 = AES
- 128-EEA3 = ZUC (soporte de momento opcional)

Mejoras:

- Características mejoradas en el nivel RRC y NAS (señalización)
- Mejor protección de los datos de identificación del usuario
- IMEI no se transmite sin protección de integridad
- Protección de datos de señalización útiles para geolocalización se transmiten cifrados
- Mejor protección de integridad
- Protección de integridad del protocolo RRC
- Protección de integridad con validez de contexto de seguridad EPS (evolved packet system → LTE)
- Soporte a cifrado (opcional) en señalización NAS y RRC

Vulnerabilidades heredadas:

- El protocolo Diameter hereda muchas de las vulnerabilidades descubiertas en los protocolos SS7
- Nuevas potenciales vulnerabilidades: La red core LTE es totalmente IP, lo cual genera nuevas vías potenciales de ataque que tienen que ser estudiadas a fondo.

8.5 ATAQUES SMS

- Ataques WAP-Push. Se envía contenido malicioso (por ejemplo, de configuración del terminal) mediante un mensaje del tipo WAP-Push. El contenido es aceptado bien sea por un error del usuario o porque el terminal

está incorrectamente configurado y acepta el contenido sin la intervención del destinatario.

- Ataques MMS Los más comunes son aquellos que envían un link a contenido malicioso destinado a explotar alguna vulnerabilidad del software del terminal

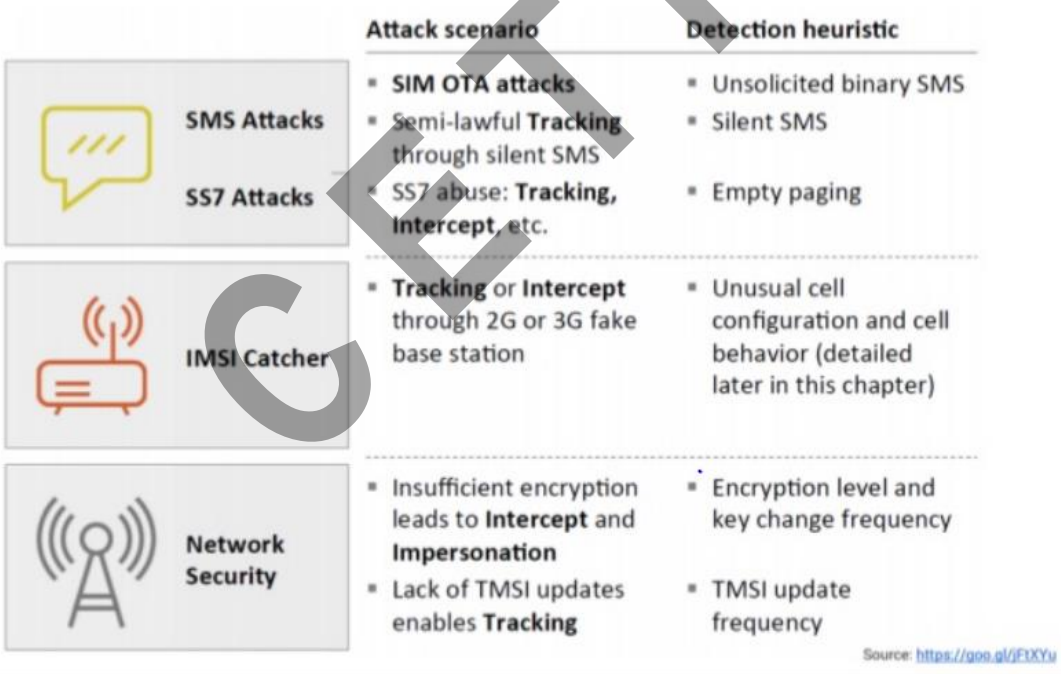
- Ataques mediante SMS en modo PDU.

  http://www.blogelectronica.com/sms-pdu/

  Se envía un SMS con contenido destinado a la SIM que consigue saltarse los controles de seguridad de la misma e instalar ese contenido.

8.6 HERRAMIENTAS:

Snoopsnitch: Aplicación capaz de recoger trazas de las redes GSM y analizarlas para detección de anomalías.
Darshak para la detección de distintos ataques (IMSI cátchers, Silent sms2, etc)



Algorithms for voice encryption:

- A5/1: the "original" unweakened GSM encryption algorithm. 64 bits. Usado en Europa y USA. Inseguro. Vulnerable por ingeniería inversa.
- A5/2: the "export variant" weakened version of A5/1. 64 bits. Se usa fuera de Europa Más inseguro que A5/1.

- A5/3: KASUMI, in use in 3G networks, stronger than A5/1. Cifrado de bloques. 64 bits de tamaño de bloque, 128 bits de tamaño de clave. También se usa para GSM, EDGE y GPRS
- A5/4: SNOW 3G, in use in 4G LTE networks. También se usa en UMTS
- A5/0: no encryption (doesn't count as encryption, here for sake of completeness only)

Algorithms for packet data encryption:

- GEA/0: no encryption, here for sake of completeness.
- GEA/1: used for GSM GPRS/EDGE/3G/4G, 64-bit keylength, 96-bit state, proprietary stream cipher. Broken, can use gprsdecode for decryption.
- GEA/2: used for GSM GPRS/EDGE/3G/4G, 64-bit keylength, 125-bit state, proprietary stream cipher. Broken, as with GEA/1 can be decoded with gprsdecode.
- GEA/3: used for GSM GPRS/EDGE/3G/4G, 64-bit keylength, 128-bit state, based off KASUMI. Limited break, as with A5/3.
- GEA/4: used for GSM GPRS/EDGE/3G/4G, 128-bit keylength, 128-bit state, based off KASUMI

9 CONCLUSIONES

En este tema se mencionan los principales centros de respuesta a incidentes que existen en España:

- CERTSI
- CCN-CERT
- IRIS-CERT

Así como herramientas como REYES o LUCIA que pone a disposición el CCN para la gestión incidentes de seguridad.

Respecto a los principales tipos de ataques en redes, se pueden clasificar en:

- Denegaciones de servicio.
- Desbordamiento de buffer.
- Fuzzing.
- Ingeniería social.
- Escuchas en red.
- Administración incorrecta de los sistemas.
- Spoofing.
- Ransomware.
- APTs.
- Ataques sobre criptomoneda.

A continuación, se describen los distintos protocolos de acceso al medio y autenticación como IPSEC en la capa IP, TLS en la capa de transporte o SAML para los servicios Web.

También se tratan los mecanismos de seguridad para el acceso a las redes Wifi.

Sobre el control de intrusiones, se describen las siguientes soluciones:

- Sistemas IDS e IPS
- Wireless IPS
- Gestores de eventos o SIEM
- Firewalls
- Otros dispositivos de seguridad como UTMs, soluciones para la prevención de fugas de información (DLP), etc.

Por último, se hace una breve descripción de los mecanismos de seguridad en las redes móviles remitiendo para más información al tema específico para el estudio de estas tecnologías.

10 REFERENCIAS

- ISO/IEC 27001:2005 - Information technology -- Security techniques
- ISO/IEC 17799:2005 - Information technology -- Security techniques
- W3C: http://www.w3c.es
- OASIS Web Services Security (WSS) TC: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss
- Software Security: Building Security in. Gary McGraw. Addison Wesley Software Security Series. 2006.
- OWASP. https://owasp.org
- Guías de Seguridad de las TIC (CCN-STIC-412, CCN-STIC-422, CCN-STIC-470G1, CCN-STIC-470G2, CCN-STIC-471D, CCN-STIC-472E, CCN-STIC-473D, CCN-STIC-454, CCN-STIC- 455, CCN-STIC-812).
- Web Services Architecture: http://www.w3.org/TR/ws-arch
- XML Encryption Syntax and Processing: http://www.w3.org/TR/xmlenc-core
- XML-Signature Syntax and Processing: http://www.w3.org/TR/xmldsig-core
- NIST SP 800-40 - Creating a Patch and Vulnerability Management Program
- NIST SP 800-83 - Guide to Malware Incident Prevention and Handling for Desktops and Laptops
- NIST SP 800-153 - Guidelines for Securing Wireless Local Area Networks (WLANs)
- NIST SP 800-94 - Guide to Intrusion Detection and Prevention Systems (IDPS)
- NIST SP 800-95 - Guide to Secure Web Services

.