Redes de Datos II
Seguridad

Luis Marrone

LINTI–UNLP

26 de noviembre de 2021

Contenidos

Notas:

Seguridad

- ✓ Seguridad en la red
- ✓ Seguridad en la Información
- ✓ Seguridad
  - Autenticidad de los datos
  - Seguridad de no interrupción del servicio
  - Seguridad frente a intrusos

Seguridad . . .

- ✓ Proteger los recursos físicos y lógicos
- ✓ Extensible a los cables, routers y todo ítem que constituya la infraestructura de la red
- ✓ La protección del recurso lógico se traduce en:
  - Integridad de los datos
  - Disponibilidad de los datos
  - Privacía

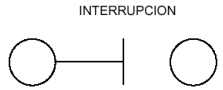
Notas:

Políticas de Seguridad

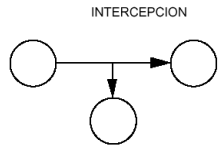
- ✓ Otorgar permisos de acceso
- ✓ Debe ser amplia:
  - Nivel de red
  - Alcanzar a la información en todas sus formas
- ✓ Cultura de seguridad

Amenazas a la Seguridad

- ✓ Interrupción
  - Parte del sistema queda destruida o no disponible
  - Destrucción hardware,corte de una línea de comunicación



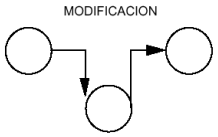
- ✓ Intercepción
  - Una entidad no autorizada accede a parte de la información
  - Pinchazo línea telefónica, copia ilícita de ficheros, intercepción vía radio comunicaciones móviles

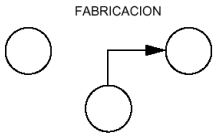


Notas:

Amenazas a la Seguridad . . .

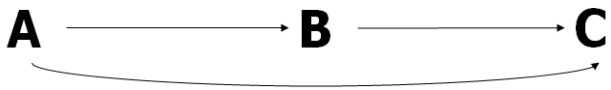
- ✓ Modificación
  - Una entidad no autorizada accede a parte de la información y modifica su contenido
  - Alteración de ficheros de datos, alteración de programas, modificación de mensajes trasmitidos por la red
- ✓ Fabricación
  - Una entidad no autorizada envía mensajes haciéndose pasar por un usuario legítimo





Seguridad e Internet

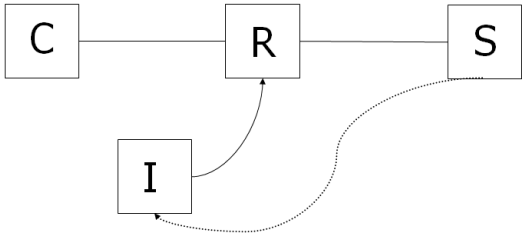
El carácter transitivo vence a la seguridad



Una organización no puede garantizar seguridad por sí sola

Notas:

Autentificación



- La Autentificación se resuelve por medio de sistemas de clave o encriptación
- La encriptación resuelve el problema de privacidad
- El emisor encripta el mensaje con la clave pública del receptor
- El receptor lo decodifica con su clave privada
- Doble codificación para autentificar los usuarios

Aclaremos

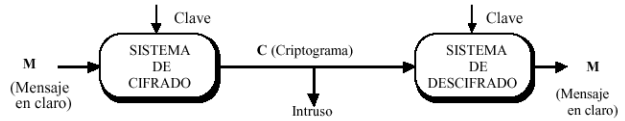
Criptografía: El arte/ciencia de cifrar un texto

Criptoanálisis: El arte/ciencia de obtener la clave o descifrar el mensaje sin conocer la clave

Criptología: Estudio de la criptografía y el criptoanálisis

Notas:

Sistemas Criptográficos



Esquema de transmisión segura de un mensaje

- ✓ Es el encargado de calcular el mensaje cifrado C, a partir del mensaje en claro M y de la "clave de cifrado"; y de realizar el proceso inverso, el descifrado, y así determinar M a partir del mensaje cifrado y la "clave de descifrado".
- ✓ Claves iguales: Algoritmos simétricos
- ✓ Claves diferentes: Algoritmos asimétricos

Transposición

- Cambia el orden de los caracteres o bits según un patrón:
  Ej: dividir el texto en bloques de 4 letras,
  REDES DE DATOS $\Longrightarrow$REDE SDED ATOS
- Tomar como patrón 4213
  EERD DDSE STAO $\Longrightarrow$ EERDDDSESTAO

Notas:

Sustitución

- ✓ Cada letra se sustituye por otra según una tabla y según su posición en el texto
- ✓ Si no depende de la posición es monoalfabética
- ✓ Si depende de la posición es polialfabética

Monoalfabética

- ✓ Julio César
- ✓ $X \Longrightarrow X + 3$

  ABCDEFGHIJKLMNOPQRSTUVWXYZ
  DEFGHIJKLMNOPQRSTUVWXYZABC

- ✓ BUENOS DIAS $\Longrightarrow$ EXHQRV GLDV

Notas:

Polialfabética

Vigenère - Alfabeto Castellano

- ✓ n coordenadas enteras en el intervalo $0 \leq x \leq 26$

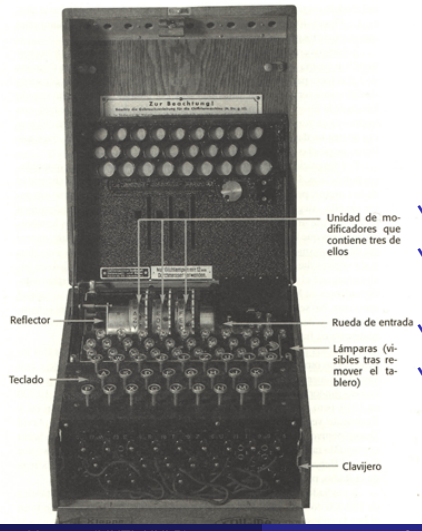
$$k = (k_0, k_1, \cdots, k_{n-1}) \textbf{ en } Z_{27}^n$$

- ✓ Se numeran las letras del texto $t_0, t_1, t_2, \cdots, t_m$
- ✓ Se sustituye t_i por c_i según:

$$c_i = (t_i + k_{i \text{ mód } n}) \text{ mód } 27$$

- ✓ Si $n = 1$, César

Rotores

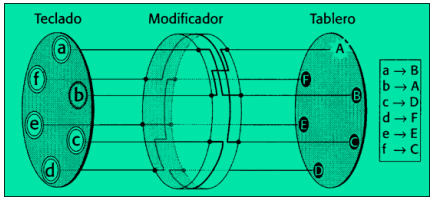


Enigma

- ✓ Creada en 1923
- ✓ Utilizada en la II Guerra Mundial por el ejército alemán
- ✓ Utiliza mecanismo de rotores
- ✓ Permite codificar/decodificar el mensaje a encriptar

Notas:

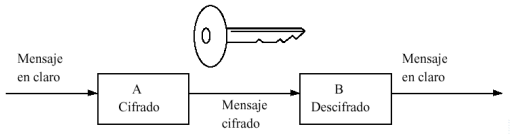
Enigma



- ✓ El rotor/modificador implementa la sustitución monoalfabética
- ✓ Al girar el rotor se compone otra sustitución monoalfabética
- ✓ Se agregan dos rotores
- ✓ Por cada cifrado el primer rotor gira una posición
- ✓ Por cada vuelta completa del primer rotor, el segundo gira una posición . . .
- ✓ La rueda de entrada y el reflector realizan sustituciones adicionales

Algoritmos simétricos

- ✓ Son los algoritmos más clásicos de encriptación
- ✓ Utilizados en redes comerciales desde el principio de los 70
- ✓ Se emplea la misma clave en las transformaciones de cifrado y descifrado
- ✓ Dos sistemas A y B desean comunicarse de forma segura, y mediante un proceso de distribución de claves, ambos compartirán un conjunto de bits que será usado como clave
- ✓ Más significativos: DES y AES
- ✓ Dos técnicas principales:
  - Cifrado en "stream"
  - Cifrado en bloque



Notas:

Cifrado en Bloque

- ✓ Utilizado en e-mail(PGP), seguridad en sesiones TCP(SSL), a nivel de red(IPSec)
- ✓ El texto plano se divide en bloques de k bits
- ✓ Cada bloque se encripta independientemente
- ✓ El cifrado consiste en "mapear" los k bits del texto plano con los k bits del texto cifrado
- ✓ Con $k = 3$ tenemos 8 posibles entradas que se permutan en $8! = 40.320$ posibilidades
- ✓ Con $k = 3$ es rápidamente criptoanalizado
- ✓ Usualmente se parte de $k = 64$, generando $2^{64}!$ permutaciones

Cifrado con $k = 3$

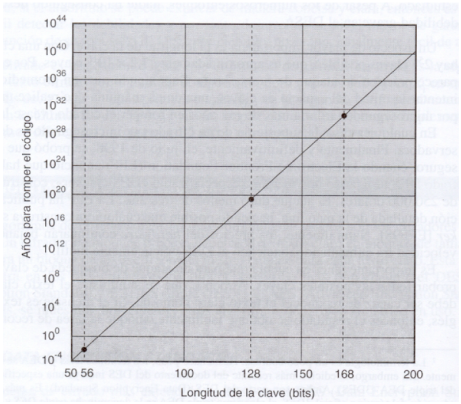
plano	cifrado	plano	cifrado
000	110	100	011
001	111	101	010
010	101	110	000
011	100	111	001

- Este esquema de tabla completa con $k = 64$ resulta muy seguro, según se ve en la próxima transparencia
- Pese a eso resulta dificultosa su implementación

Notas:

Criptografía

Tiempo de Criptoanálisis



Tiempo empleado en romper un código
(Suponiendo $10^6 descifrados/\mu s$)

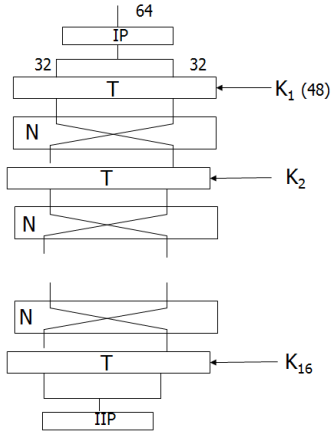
Criptografía

Data Encryption Standard – DES

- ✓ Nació como petición del gobierno de los EEUU al "National Bureau of Standards" en 1973 para poder mantener comunicaciones seguras
- ✓ Se eligió uno presentado por IBM y tras una serie de revisiones públicas, fue adoptado como estándar en 1977
- ✓ El algoritmo se basa en permutaciones, substituciones y sumas módulo 2
- ✓ Emplea una clave de 56 bits y opera con bloques de datos de 64 bits
- ✓ Utiliza funciones que simulan la permutación aleatoria de tabla completa
- ✓ Con la tecnología de esa época hubieran tardado 2200 años en probar todas las posibles claves. Hoy sólo se tarda 1 segundo!!!!

Notas:

DES



- IP: sustitución fija de 64 en 64 bits
- IIP: inversa de la anterior
- T: Transformación con clave de 48 bits. Preserva la mitad derecha
- N: "swap" de las mitades
- K_i: claves de 48 bits, derivadas de la original

Triple DES – 3DES

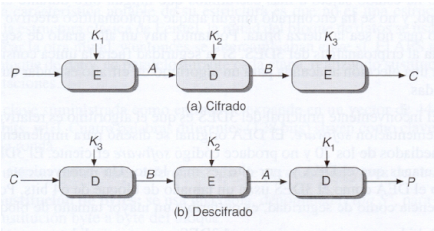
- ✓ Se estandarizó inicialmente para aplicaciones financieras en el estándar ANSI X9.17 en 1985.
- ✓ Se incorporó como parte del DES en 1999, con la publicación de FIPS PUB 463
- ✓ Usa tres claves y tres ejecuciones del algoritmo DES. La función sigue la secuencia cifrar-descifrar-cifrar(EDE: encrypt-decrypt-encrypt)

$$C = EK_3[DK_2[EK_1[P]]]$$

Donde
C = texto cifrado
P = texto plano
$E_K[X] =$
cifrado de X usando la clave K
$D_K[Y] =$
descifrado de Y usando la clave K

Notas:

3DES



- ✓ El descifrado del segundo paso no es significativo en términos criptográficos
- ✓ Su única ventaja es que permite a los usuarios del 3DES descifrar datos cifrados por usuarios del DES:

$$C = E_{K_1}[D_{K_1}[E_{K_1}[P]]] = E_{K_1}[P]$$

- ✓ Resulta una clave de 168 bits

Advanced Encryption Standard – AES

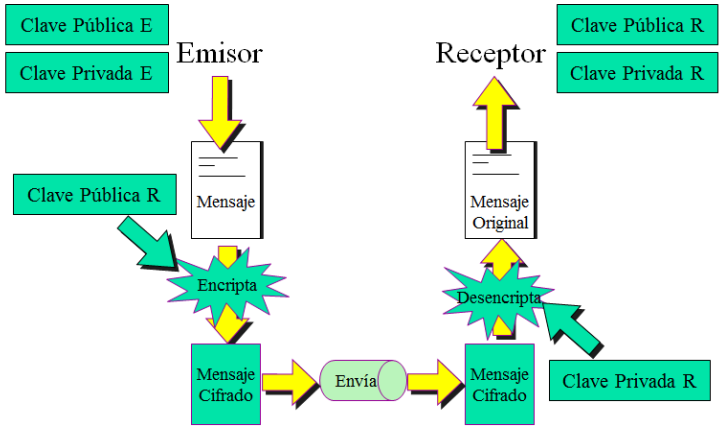
- ✓ Publicado el 2 de Octubre de 2000 por el NIST como ganador de la convocatoria AES (estándar de cifrado avanzado)
- ✓ Sustituye al D.E.S.
- ✓ El tamaño de clave debe ser de, al menos, 128, 192 y 256 bits (debe admitir los tres), y el tamaño de bloque de cifrado debe ser de 128 bits
- ✓ Buena combinación de seguridad, velocidad, eficiencia (en memoria y puertas lógicas), sencillez y flexibilidad

Notas:

Algoritmos Asimétricos

- ✓ Son aquellos que emplean dos claves, una pública y otra privada
- ✓ La clave privada sólo la posee el receptor y la utiliza para desencriptar
- ✓ La clave pública la posee el receptor, pero se la pasa al emisor para que la utilice a la hora de encriptar su mensaje
- ✓ Son más seguros, ya que aunque un intruso consiga la clave pública, no será capaz de encontrar la clave privada a través de la clave pública para poder desencriptar el mensaje
- ✓ El principal inconveniente es que resulta computacionalmente costosa su implementación
- ✓ Son más lentos que los algoritmos simétricos

Algoritmos Asimétricos . . .



Notas:

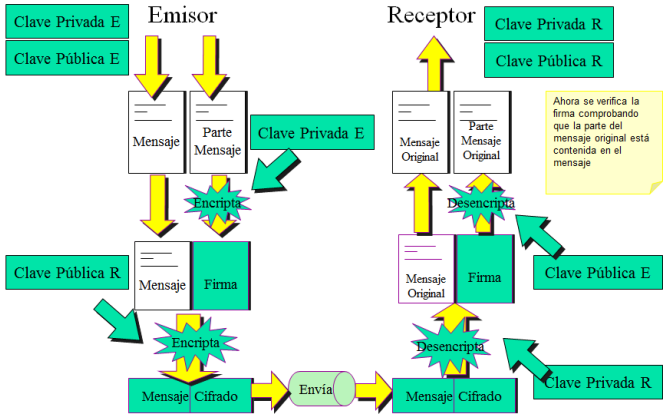
Criptografía

RSA

- ✓ Es el algoritmo asimétrico más sencillo de comprender e implementar
- ✓ Su nombre proviene de sus tres inventores: Rivest, Shamir y Adleman
- ✓ Se basa en la dificultad para factorizar números grandes, así pues, las claves se calculan a partir de un número que se obtiene como producto de dos números primos grandes
- ✓ Algoritmo utilizado en el SSH (Secure Shell Client)
- ✓ Un tamaño de clave de 1024 bits (300 dígitos decimales aproximadamente) se considera lo suficientemente robusto para casi todas las aplicaciones

Criptografía

RSA – Firma Digital



Notas:

Algoritmo RSA

Generación clave

Seleccionar p, q	p y q primos, $p \neq q$
Calcular $n = p \times q$	
Calcular $\phi(n) = (p-1)(q-1)$	
Seleccionar entero e	$gcd(\phi(n), e) = 1;\ 1 < e < \phi(n)$
Calcular d	$de \bmod \phi(n) = 1$
Clave pública	$KU = \{e, n\}$
Clave privada	$KR = \{d, n\}$

Cifrado

Texto claro:	$M < n$
Texto cifrado:	$C = M^e \pmod n$

Descifrado

Texto cifrado:	C
Texto claro:	$M = C^d \pmod n$

RSA – Ejemplo

- ✓ Manolito envía un mensaje encriptado a Mafalda
- ✓ Mafalda adopta $p = 5$; $q = 7$ (para facilitarle las cuentas a Manolito), por lo tanto:
  $n = 35$ y $z = 24$,
- ✓ Mafalda elige:
  $e = 5$; 5 y 24 son primos entre sí(e clave pública de Mafalda)
  $d = 29$; (5×29) mód $24 = 1$, d clave privada de Mafalda
- ✓ El mensaje de Manolito consta de 4 palabras "JELP"

texto plano	Codif	m^e	texto cifrado $c = m^e$ mód n
J	12	248832	17
E	15	759375	15
L	22	5153632	22
P	5	3125	10

Notas:

RSA – Ejmplo . . .

- ✓ El mensaje llega y Mafalda aplica el algoritmo para desencriptar

texto cifrado	c^d	$m = c^d$ mód n	texto plano
17	48196857210675091509150914118252230716 97	12	J
15	12783403940394885893911123275756835937 5	15	E
22	85164331908653770195619449972110603059 2	22	L
10	10000000000000000000000000000000	5	P

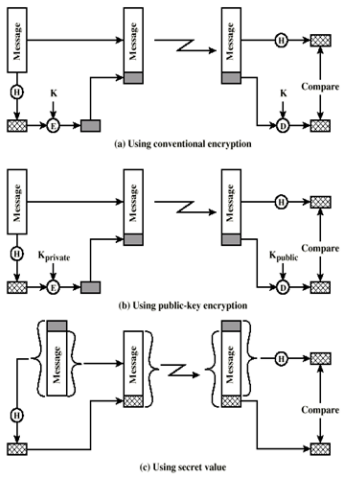
Funciones de Hashing

- ✓ No tienen inversa
- ✓ Dado H(T) es imposible encontrar T
- ✓ Dado T no se puede encontrar T'tal que H(T) = H(T'); computacionalmente inviable
- ✓ MD5 (RFC 1321) 128 bits de hashing
- ✓ SHA-1(FIPS 1995)160 bits de hashing. Desestimada en 2011
- ✓ SHA-2, SHA-3

Notas:

Criptografía

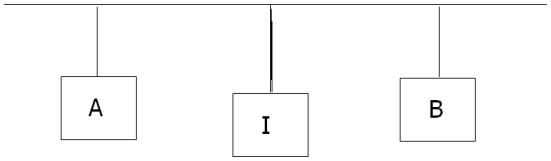
Autentificación - Firma - Hashing



Extraído de "Data and Computer Communications". W. Stallings, 9a Edición

Ataques

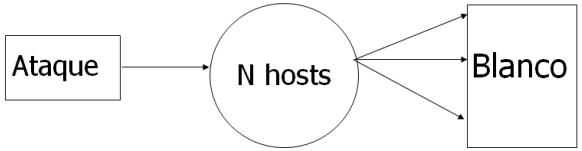
ARP



- ✓ ARP – Stateless
- ✓ I envía replies falsos
  Orig: IP(B), HA (I)
  Dest: IP(A), HA(A)
- ✓ I deshabilita ARP para esconderse
- ✓ Inhabilita el envío de A a B
- ✓ UNIX: Si A contiene equiv B, se hace rlogin a A

Notas:

ICMP



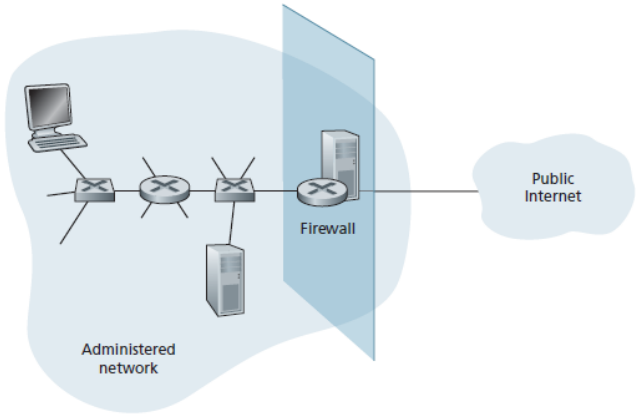
- ✓ Ataque ICMP echo request
  Origen: IP(T)
  Destino: Broadcast (N)
- ✓ Cada host le manda un ICMP reply al Blanco

Características

- ✓ Combinación de hardware y software que aísla la red interna de una organización de una red pública como Internet
- ✓ Todo el tráfico, entrante y saliente atraviesa el firewall
- ✓ Sólo el tráfico autorizado según las políticas de seguridad local lo atraviesa
- ✓ El firewall es inmune a los ataques
- ✓ Implementado en base a filtrado de datagramas

Notas:

Red con Firewall



Extraído de Kurose-Ros, *Computer Networking - A Top-Down Approach*

Filtros de Firewall

- ✓ Dirección IP origen y/o destino
- ✓ Tipo de protocolo:TCP, UDP, ICMP, OSPF, . . .
- ✓ Puerto TCP o UDP origen y/o destino
- ✓ Flags de TCP: SYN, ACK, . . .
- ✓ Tipo de mensaje ICMP
- ✓ Diferentes reglas para datagramas entrantes y salientes de la red interna
- ✓ Diferentes reglas para diferentes interfaces de los routers
- ✓ Implementadas a través de listas de acceso en los routers
- ✓ Filtrado positivo/negativo

Notas:

Filtrado Negativo

acción	dir. origen	dir. destino	protocolo	port orig	port dest.	flag
Si	140.23.0.0/16	fuera de 140.23.0.0/16	TCP	> 1023	80	–
Si	fuera de 140.23.0.0/16	140.23.0.0/16	TCP	80	> 1023	ACK
Si	140.23.0.0/16	fuera de 140.23.0.0/16	UDP	> 1023	53	–
Si	fuera de 140.23.0.0/16	140.23.0.0/16	UDP	53	> 1023	–
No	todo	todo	todo	todo	todo	todo

Objetivos

RFC 4301

"IPsec is designed to provide interoperable, high quality, cryptographically-based security for IPv4 and IPv6"
En el marco de IP, es decir a nivel de red

Consta de dos protocolos de seguridad en el tráfico de datos

- Authentication Header (AH)
- Encapsulating Security Payload(ESP)

Y un protocolo y procedimientos para la distribución de claves.

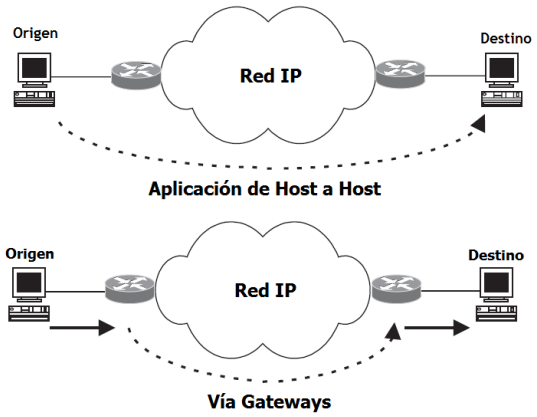
- Internet Key Exchange(IKEv2)

Notas:

Características de IPsec

- IP Authentication Header (AH) ofrece integridad y autentificación del origen
- Encapsulating Security Payload (ESP) ofrece el mismo conjunto de servicios y también confidencialidad.
- Ambos AH y ESP ofrecen control de acceso con el complemento de los procedimientos de distribución de claves y administración de flujo de tráfico.
- Se pueden aplicar individualmente o combinados.
- Cada uno de ellos soporta dos modos de uso:
  - Modo Transporte:Proveen protección para el nivel superior.
  - Modos Túnel: Aplican a túneles de IP.

Esquema – Alcances



Notas:

Security Association I

- ✓ Relación unidireccional entre transmisor y receptor
- ✓ Contiene el esquema de seguridad adoptado
- ✓ Dicho esquema puede ser AH o ESP pero no ambos
- ✓ Si se emplean ambos entonces se deben crear dos SAs
- ✓ Es una conexión "simplex" que provee servicios de seguridad al tráfico que transporta
- ✓ Para asegurar una comunicación típica (bidireccional) entre dos IPsecs se requiere un par de SAs, una en cada dirección
- ✓ Administradas por el protocolo IKE
- ✓ IKE las crea explícitamente dada la modalidad usual de transmisión de datos

Security Association II

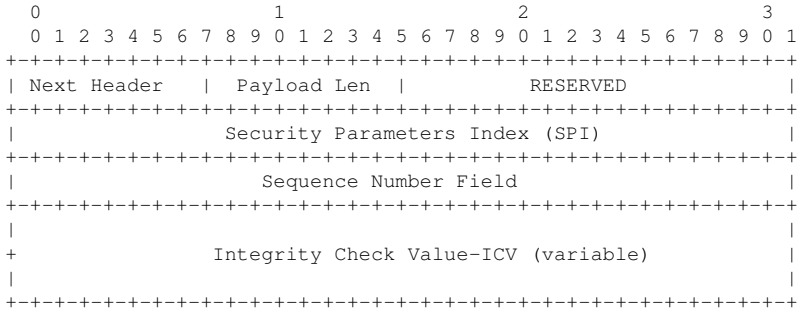
- ✓ Especificada por:
  - SPI(Security Parameter Index): Identificador asignado a la SA
  - Transportado en el header del AH o ESP
- ✓ Se le puede agregar:
  - Security Protocol Identifier: indica si es AH o ESP
  - Dirección IP destino
  - Dirección IP origen

Notas:

IPSec – AH

- ✓ IP Authentication Header (AH) provee integridad y autentificación de datagramas IP
- ✓ AH provee autentificación del header, dentro de lo posible, y del payload correspondiente
- ✓ Los campos del header que cambian en el trayecto y que el receptor no pueda predecir quedan fuera del alcance de la autentificación
- ✓ La autentificación es parcial
- ✓ RFC 4302

AH – Estructura I



Notas:

AH – Estructura II

- ✓ Next Header:
  - Identifica el payload que está a continuación de él
  - 4 para IPv4
  - 41 para IPv6
  - 6 para TCP
  - Códigos provistos por el IANA
- ✓ Payload Length:
  - Longitud del AH en palabras de 32 bits menos 2
  - Si el cálculo del ICV dio 96 bits, entonces este campo tendrá el valor 4 (3 para la primera parte de AH y 3 para el ICV - 2)
  - Para IPv6 se da en palabras de 8 bytes
- ✓ Reserved:
  - Para uso futuro
  - Se rellena con ceros
  - Ignorado por el receptor

AH – Estructura III

- ✓ Security Parameters Index (SPI)
  - Utilizado por el receptor para identificar la SA a la cual corresponde
  - Valores entre 1 y 255 reservados para el IANA
  - Valor 0 de uso local. No debe aparecer en un datagrama transportado por la red
- ✓ Sequence Number
  - Contador incializado en 0 al crearse una SA
  - Se incrementa en 1 por cada paquete enviado
  - No recicla. Antes de enviar el paquete 2^{32} se debe crear una nueva SA
  - Extensión a 64 bits. Se negocia al establecer la SA. Se transmiten los 32 menos significativos
  - Se consideran los 64 para el cálculo del ICV

Notas:

AH – Estructura IV

- ✓ ICV
  - El algoritmo empleado está especificado por la SA
  - Pueden ser basados en:
    - Algoritmos simétricos, AES, 3DES
    - Funciones HASH, MD5, SHA-1, SHA-256, etc

El IP Header contendrá el valor 51 en el protocol type, que identifica a IPSec.
Next header contendrá por ejemplo 6 para identificar a TCP, 4 para IPv4, 41 para IPv6
Payload length: Ojo!!!, es la longitud del AH header solamente.
El SPI es el de que hablamos en las SA.
El sequence number se inicializa en 0 al comenzar la sesión y se incrementa por cada paquete enviado. NO recicla. Al agotarse debe establecerse una nueva sesión.
Authentication Data: Contiene el mensaje de autentificación para el paquete. Se lo llama también Integrity Check Value, ICV.
Este campo se calcula sobre:
Campos del IP header que no cambian en el trayecto o que son predecibles en la llegada. Los que no cumplen esto se colocan en 0 para el cálculo.
El header de AH excepto él mismo. Se considera 0.
El payload del datagrama original íntegro.
El cálculo es el resultado de aplicar una función de Hashing.

La longitud es variable, dependiendo de la función de hashing utilizada, pero no puede ser mayor a 96 bits.

Notas:

ICV – Clasificación de Campos – IPv4

Immutables

- Version
- Internet Header Length
- Total Length
- Identification
- Protocol (El código de AH)
- Source Addres
- Destination Address (sin loose o strict source routing)

Mutables pero predecibles

- Destination Address (con loose o strict source routing)

Mutables (puestos en 0 para el cálculo de ICV)

- TOS
- Flags
- Fragment Offset
- Time to Live (TTL)
- Header Checksum

ICV – Clasificación de Campos – IPv6

Immutables

- Version
- Payload Length
- Next Header
- Source Address
- Destination Address (sin Routing Extension Header)

Mutables pero predecibles

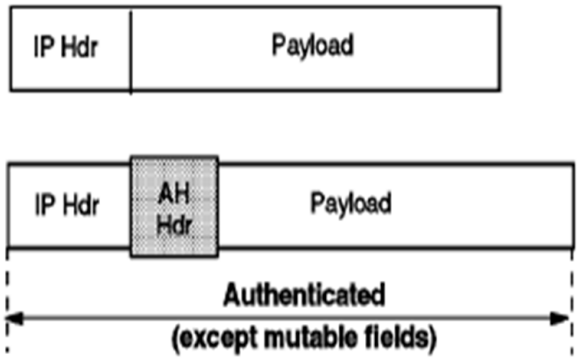
- Destination Address (con Routing Extension Header)

Mutables (puestos en 0 para el cálculo de ICV)

- CoS
- Flow Label
- Hop Lim

Notas:

AH – Modo Transporte



AH – Modo transporte completo – IPv4

RFC 4302

```
                BEFORE APPLYING AH
               ----------------------------
       IPv4    |orig IP hdr  |     |      |
               |(any options)| TCP | Data |
               ----------------------------
                AFTER APPLYING AH
               ------------------------------------------------------
       IPv4    |original IP hdr (any options) | AH | TCP |    Data   |
               ------------------------------------------------------
               |<- mutable field processing ->|<- immutable fields ->|
               |<----- authenticated except for mutable fields ----->|
```


Notas:

AH – Modo transporte completo – IPv6

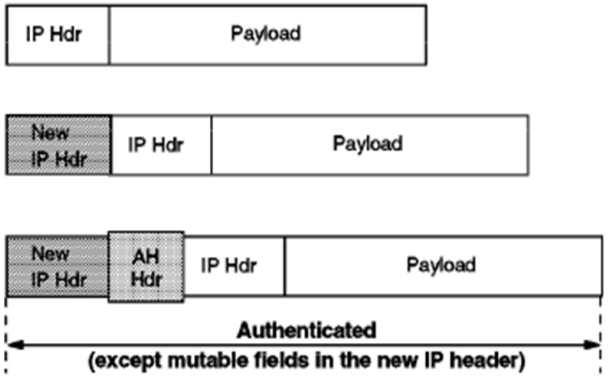
RFC 4302

```
                    BEFORE APPLYING AH
                 ----------------------------------------
          IPv6   |             | ext hdrs |     |      |
                 | orig IP hdr |if present| TCP | Data |
                 ----------------------------------------

                    AFTER APPLYING AH
                 ------------------------------------------------------------
          IPv6   |             |hop-by-hop, dest*, |     | dest |     |      |
                 |orig IP hdr  |routing, fragment. | AH  | opt* | TCP | Data |
                 ------------------------------------------------------------
                 |<--- mutable field processing -->|<-- immutable fields -->|
                 |<---- authenticated except for mutable fields ----------->|

                      * = if present, could be before AH, after AH, or both
```

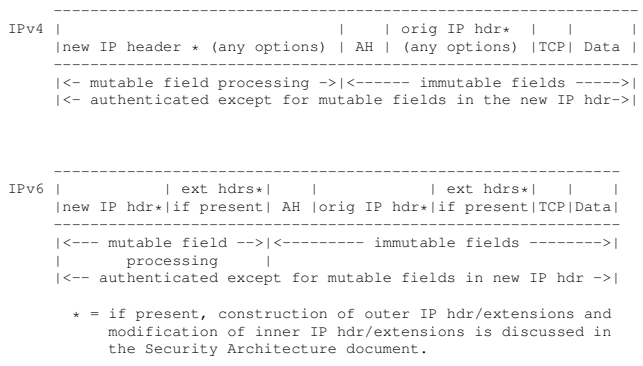

AH – Modo Túnel



Notas:

AH Modo Túnel completo

RFC 4302

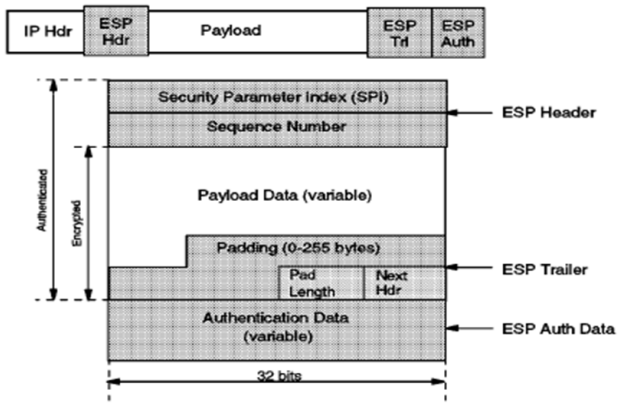


Encapsulated Security Payload – ESP

- ✓ ESP está diseñado para proveer servicios de seguridad en IPv4 e IPv6
- ✓ Puede aplicarse sólo o en combinación on AH o en forma anidada
- ✓ Las SA pueden proveerse:
  - Entre hosts
  - Entre gateways
  - Entre gateway y host
- ✓ El header de ESP se aloja:
  - Después del header de IP y antes del payload del datagrama original(Modo transporte)
  - Antes del header de un datagrama IP encapsulado
- ✓ RFC 4303

Notas:

ESP – Estructura



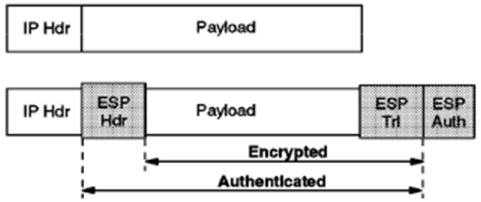
Está identificado por protocol type 50.
La autentificación es opcional.
El padding surge porque la encriptación se realiza en la modalidad bloque y pueden faltar bytes para completar el tamaño del bloque que utiliza el algoritmo de encriptación.
El pad length es un campo de 8 bits.
El next header es un campo de 8 bits.

Notas:

ESP – Características

- ✓ Presenta dos modalidades de servicio
- ✓ Autenticación: abarca todo el datagrama
- ✓ Encriptación: Abarca el payload
- ✓ La semántica de los campos es similar a la de AH
- ✓ La diferencia es que en encriptación el campo ICV carece de significado

ESP – Modo Transporte



Notas:

ESP – Modo Transporte(Detalle)

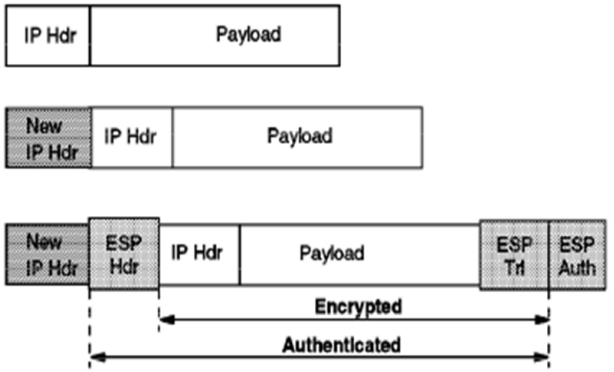
RFC 4303

```
                BEFORE APPLYING ESP
          ----------------------------------------
IPv6      |             | ext hdrs |     |      |
          | orig IP hdr |if present| TCP | Data |
          ----------------------------------------

                AFTER APPLYING ESP
          ------------------------------------------------------------
IPv6      | orig |hop-by-hop,dest*,|   |dest|   |     | ESP    | ESP|
          |IP hdr|routing,fragment.|ESP|opt*|TCP|Data|Trailer| ICV|
          ------------------------------------------------------------
                                    |<--- encryption ---->|
                                  |<------ integrity ------>|

              * = if present, could be before ESP, after ESP, or both
```

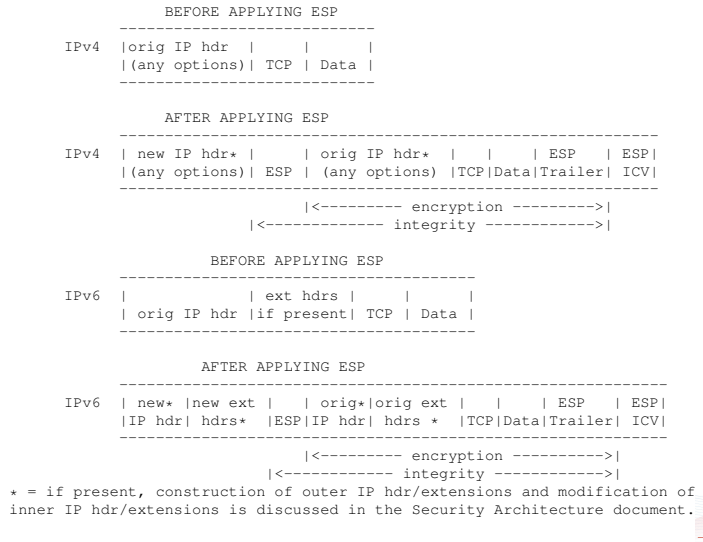

ESP – Modo Túnel



Notas:

ESP – Modo Túnel(Detalle)

RFC 4303



* = if present, construction of outer IP hdr/extensions and modification of inner IP hdr/extensions is discussed in the Security Architecture document.

IPSec – Administración

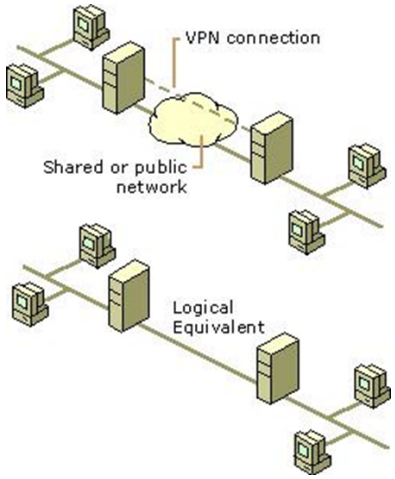
- ✓ Internet Key Exchange v2 (IKEv2)
- ✓ RFC 5996 (4306)
- ✓ Los servicios definidos por IPsec deben ser provistos y mantenidos a través de un control de estados que de hacerlo en forma manual resultarían poco escalables
- ✓ IKEv2 automatiza ese proceso
- ✓ Actualiza ISKAMP(Internet Security Association and Key Management Protocol-RFC 4306) y protocolos relacionados

Notas:

Características

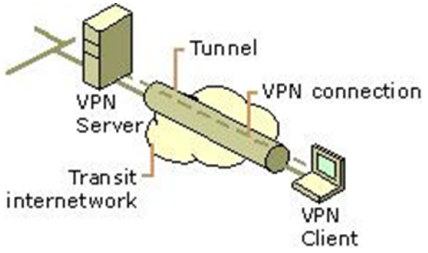
- ✓ Aprovechar la capacidad de interconexión de Internet
- ✓ Funcionar como una red privada
- ✓ Reducción de costos
- ✓ Escalabilidad
- ✓ Tunneling
- ✓ Encriptación

Arquitectura



Notas:

Elementos I



- ✓ VPN client. El computador que inicia la conexión VPN a un VPN Server. El cliente normalmente es una PC o router que obtiene un acceso remoto
- ✓ También pueden ser clientes PPTP o L2TP
- ✓ VPN server. El computador que acepta conexiones VPN de clientes. Puede proveer acceso remoto o ruteado

Elementos II

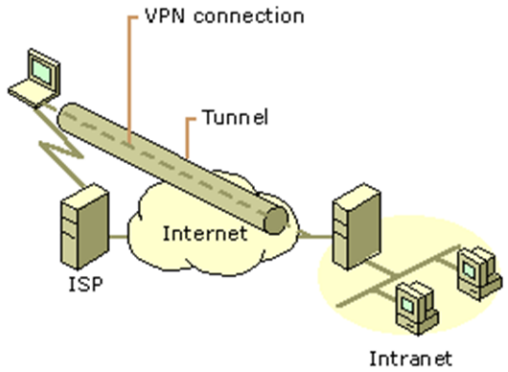
- ✓ Túnel. La etapa de la conexión en la que se encapsulan los datos
- ✓ VPN connection. La etapa de la conexión en la que se encriptan los datos. Para conexiones seguras los datos se encriptan y encapsulan en la misma etapa de la conexión.
- ✓ Si bien los datos pueden encapsularse y no encriptarse, en ese caso no estamos en presencia de una VPN
- ✓ Tunneling protocols. Estándares para manejar los túneles y encapsular los datos, como PPTP y L2TP
- ✓ Transit internetwork. La red pública o compartida por la que viajan los datos encapsulados

Notas:

Conexiones

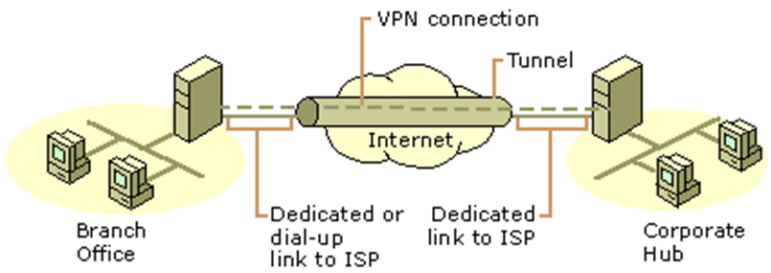
- ✓ Acceso Remoto
  - Característica individual
  - El cliente se conecta a una red privada virtual
- ✓ VPN – Ruteadas. Router - to - Router
  - Realizada por el Router
  - Interconecta dos partes de una red privada

Conexiones basadas en Internet – Acceso Remoto

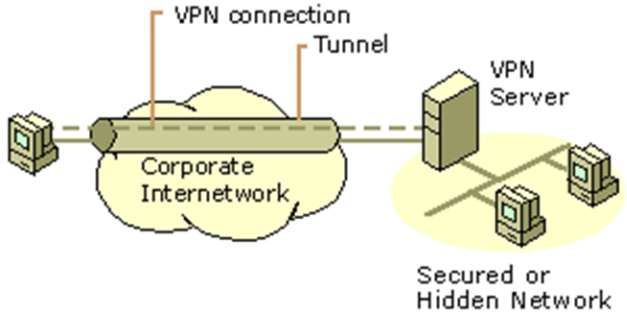


Notas:

Conexiones basadas en Internet – Ruteadas



Conexiones basadas en Intranet – Acceso Remoto



Notas:

Tecnologías VPN

- ✓ PPTP: Point-to-point-tunneling-protocol
- ✓ L2F: Layer-2-forwarding
- ✓ L2TP: Layer-2-tunneling-protocol
- ✓ IPSec: IP security protocol

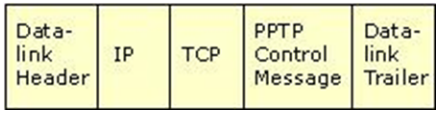
PPTP - Microsoft

- ✓ RFC 2637
- ✓ Utiliza:
  - Conexión TCP de control
  - Versión modificada de GRE(Generic Routing Encapsulation)
  - Autentificación de PPP
    - MS-CHAP(Microsoft Challenge Handshake Authentication Protocol)
    - PAP(Password Authentication Protocol)
- ✓ Hereda la compresión y/o encriptación de PPP

Notas:

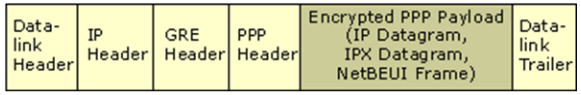
PPTP – Mantenimiento del Túnel

- Conexión TCP:
  - Cliente :port efímero
  - Servidor:port 1723
- Transmisión de Echo-request y replies



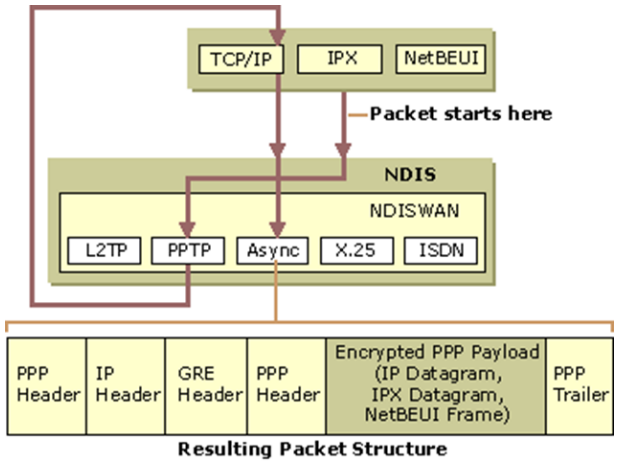
PPTP – Túnel de Datos

- ✓ Diferentes niveles de encapsulamiento
- ✓ GRE: protocol type 47
- ✓ RFC 1701 y 1702



Notas:

PPTP – Túnel de Datos . . .



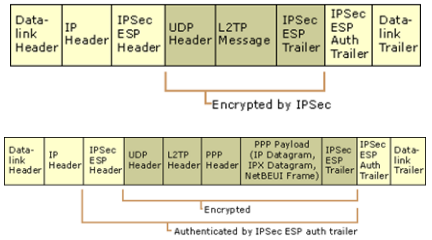
Resulting Packet Structure

Se genera un Datagrama IP y se envía a la interfase virtual que representa la conexión VPN utilizando NDIS(Network Driver Interface Specification).
NDIS lo envía a NDISWAN que lo encripta y/o comprime y lo convierte en PPP.
NDISWAN lo envía al driver de PPTP que encapsula el PPP con un header GRE.
PPTP lo envía a al driver TCP/IP.
TCP/IP encapsula los datos PPTP tunelizados con un header IP y envía el resultado a la interfase correspondiente. En el ejemplo a Async.

Notas:

L2TP – IETF

Autentificación como en PPP
Paquetes de control y datos misma estructura



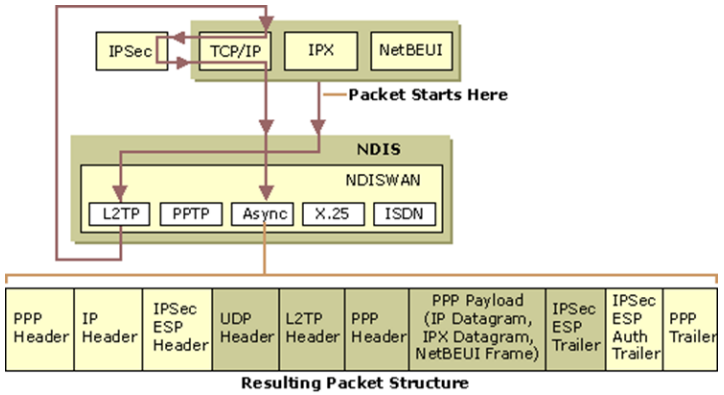
L2TP

- ✓ RFC 5641. L2TPv3
- ✓ Encapsula tramas PPP
- ✓ Envíos a IP, Frame Relay o ATM
- ✓ Especificada sobre IP
- ✓ Se encapsula en datagramas UDP
- ✓ Mantenimiento
- ✓ Datos
- ✓ Encriptación por IPsec ESP
- ✓ Múltiples sesiones por cada túnel

Notas:

Virtual Private Networks – VPNs

L2TP – Datos



El datagrama IP es enviado a la interfase virtual que representa la conexión VPN utilizando NDIS.
NDIS lo envía a NDISWAN que opcionalmente comprime y provee un header PPP.
NDISWAN envía el frame PPP al driver L2TP que agrega el header L2TP al frame PPP. En este nuevo header se incluyen las identificaciones del Call y del Túnel.
L2TP lo envía al driver TCP/IP con la información de enviarlo como segmento UDP del port 1701 al 1701 y las direcciones IP del VPN client y VPN server.
El driver TCP/IP lo pasa al driver IPSec. El protocol type del IP original se cambia a 50 para identificar a IPSec.
IPSec lo devuelve a TCP/IP quien lo envía a la interfase adecuada, (EJ: Async) en NDISWAN.
NDISWAN provee headers y trailers PPP.

Notas:

Documentación de Referencia y Consulta

- Kent, S.; Seo, K., "Security Architecture for the Internet Protocol", RFC 4301, December 2005.
- Kent, S., "IP Authentication Header(AH)", RFC 4302, December 2005
- Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, December 2005.
- Kaufman, C., Ed., "The Internet Key Exchange (IKEv2) Protocol", RFC 5996, September 2010. Actualizaciones 5998(2010/09) y 6989(2013/07)
- CSRC, "Security Requirements for Cryptographic Modules", FIPS PUB 140-2
- AES, https://doi.org/10.6028/NIST.FIPS.197
- Centros de Incidentes:
  http://www.cespi.unlp.edu.ar/cert
  https://www.redlink.com.ar/servicio_csirt.html
  https://cert.ar

Notas: