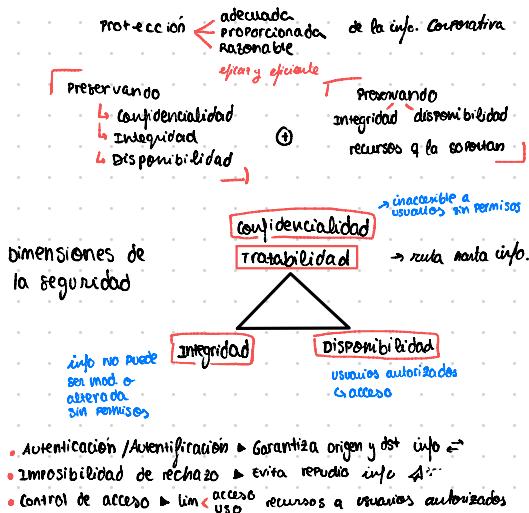




# T2: IPSEC

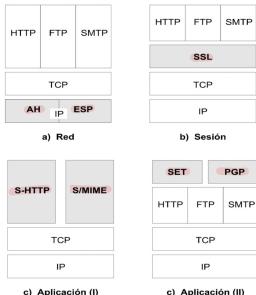
## Seguridad de la información



### Mecanismos de seguridad

- Cifrado:** alteración info (no reconocible)  $\rightarrow$  reversible en el dst
- Firma digital:** secuencia binaria q se adjunta al dst  $\Rightarrow$  receptor verifica
- Integridad de datos:** (para la protección de bloques)
  - Se adjunta secuencia cifrada obtenida a partir datos (huella digital o MAC: Message Authentication Code)
  - Para la protección de un  $\square$  ( $N$  bloques) se usa encañamiento criptográfico (se usan  $N$  bloques secuenciales y se usa encañamiento criptográfico sellos de  $\square$ )

### Ubicación de los mecanismos de seguridad



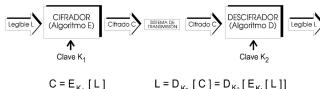
### Requerimientos de Seguridad

Tipo de sistema	Uso comercial	Sistemas clasificados
Clave simétrica	$\geq 128$	$\geq 256$
Clave pública	$\geq 1024$	$\geq 2048$

???

- Pruebas de identidad:**  $\Leftrightarrow$  info. entre los interlocutores (normalmente mediante técnicas intercambios)  $\rightarrow$  fuerza verificación q cada extremo es qdile ser [sorprenderse] autentificación [control de acceso]
- Entidades Federativas:** entidades seguras q donde los usuarios depositan  $\rightarrow$  su confianza
- Asumen papel: intermedios (actuando como notarios del internet)

### Modelo de cifrado



Algoritmos q gozan de privacidad  $\Rightarrow$  reducir claves!

En función del valor q tienen  $m$  y  $n$ :

- Sist. simétricos:** de clave priv. o única  $K_1 = K_2 = K$
- Para  $m$  posibles interlocutores:  $\frac{m(m-1)}{2}$  claves
- Problema: distrib. de claves
- Sist de clave Pública o asimétrica:**  $K_1 \neq K_2$

Para  $m$  interlocutores: sin claves permite implementar autenticación

### Cifrado simétrico

- Algoritmos: conocidos y muy eficientes  $\rightarrow$  seguridad: reside en longitud de la clave 64, 128, 1024, 256 bits
- Algoritmos: DES, 3DES, AES, IDEA, BlowFish, CAST, S/UP JACK, RC4 (fijo)

- Inconvenientes  $\leftarrow$  Distrib. larga de la clave  $\rightarrow$  Clave pública num claves  $\leftarrow \frac{m(m-1)}{2}$  Resolución entre interlocutores

### Cifrado de clave Pública (clave asimétrica)

cada interlocutor  $\rightarrow$  pareja de claves reversible obtenidas en el = proceso de generación

$$E_{K_1}[E_{K_2}[L]] = L$$

- seguridad computacional: a partir de  $m$  no puedes saber  $n$  o al revés requiere claves de longitud suficiente (2048, 4096 bits, ...)
- 2 claves  $\rightarrow$  otra se da a conocer públicamente (llave pública)
- Algoritmos: RSA, DSA, ElGamal, ...
- Inconveniente: G de proceso

### sistemas híbridos o mixtos

Combinan técnicas asimétricas y simétricas

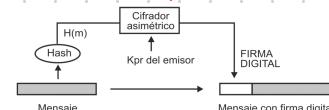
sin doble encriptación ofrecer confidencialidad e integridad de forma eficiente

### Firma digital

permite autenticar al emisor y garantizar integridad

- Utiliza modelo cifrado asimétrico:
- Se cifra con clave privada  $\rightarrow$  un residuo del emisor de longitud fija [falso positivo]

se adjunta residuo al firma digital



### Funciones hash

funciones unidireccionales  $\rightarrow$  aceptan  $m \rightarrow$  devuelven residuo

propiedades:

- H(m) debe ser computacionalmente eficiente
- debe evitar colisiones:
  - Dado  $m \rightarrow$  difícil encontrar  $m$  q verifique  $H(m)$
  - Dado  $m_1$  con  $H_1 \xrightarrow{\text{definición}} m_2$  con  $H_2$
  - Difícil  $\rightarrow m_1, m_2 \rightarrow$  residuo  $H$

### Algoritmos hash

- MD5 (Message-Digest 5): genera residuo 128 b  $\rightarrow$  somete  $f$  a bloques 512 b deseo (8 iteraciones)  $\rightarrow$  16 interacciones  $f$  con  $g$
- SHA-1 (Secure Hash Algorithm): residuos de 160 b  $\rightarrow$  operando con bloques 512 b
- Otros: SHA-X (residuos 224, 256, ...), RIPEMD-160, FOFK - 256, ...

# T2 : IPSEC

## (Seguridad de la info.)

### Gestión de claves. Certificados

Sist. clave Asimétrica

cada 2 → debe darse conocimiento mutuo



**Problema** → Puede suplantar identidad

→ obviando a conocer la clave pública falsificada

**Solución** → Autenticar la clave Pública de los usuarios

en un organismo de confianza → Autoridad de Certificación (CA)

emite documentos electrónicos, certificados, ... con la asociación [Usuario, NIF]

digitalmente firmados CA

### servicios proporcionados

	AH	ESP	ESP con autenticación
Negociación del contexto de seguridad	✓	✓	✓
Integridad de los mensajes	✓		✓
autenticación del origen de datos		✓	✓
Detectar repetición de paquetes	✓	✓	✓
Confidencialidad de la información	✓		✓
Confidencialidad del flujo intercambiado		✓	✓

## IPSec

proporciona servicios de seguridad → protocolo IP exteriorizado e integrado en IPv6

- Proporciona **autenticidad** en los extremos
- **integridad + confidencialidad** en los intercambios
- Suministra la negociación de algoritmos criptográficos de **cifrado** y **integridad**
- Componentes fundamentales:
  - Protocolos de seguridad: AH (Authentication Header)
  - ESP (Encapsulating Security Payload)
  - Asociaciones de seguridad: SA (Security Associations)
  - Intercambio de claves IKE (Internet Key Exchange)
  - Algoritmos de autenticación y cifrado (DES, AES, SHA-1, ...)

### Modos de operación

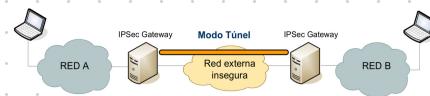
#### Modo Transporte

- Comunicación directa entre hosts (IPsec presente en **host finales**)
- La carga útil del datagrama (Payload)
- Comunicación segura **de extremo a extremo**



#### Modo túnel

- Comunicación entre los Sist. Intermedios (IPsec → no ext. finale)
- Comunicación **sólo** en el túnel
- **Todos** los campos del datagrama original (**encapsulado**)
- Permite implementar VPNs



### Authentication Header (AH)

• **integridad** → autenticación de los datagramas IP intercambiados (cabecera y datos)

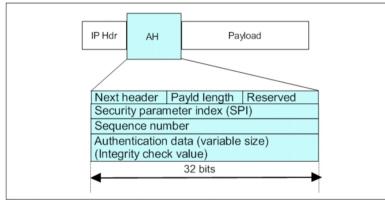
• Inserta **cabecera autenticación AH** entre: **cabecera IP extensor** y **datos transportados**

• Next header o Protocol = 51

↳ Dentro **cabecera AH** se indica naturaleza datos de la capa superior

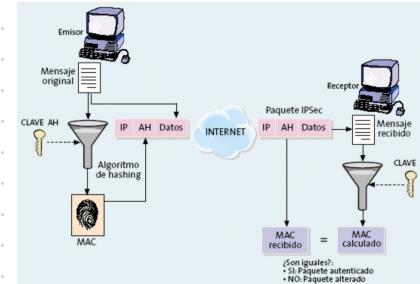
• Operación: se obtiene resultado (Hash) **usando** clave simétrica → **introducir** en **cabecera AH** → **Al saber:** huella digital, MAC o ICV (Integrity Check Value)

• Para obtener ICV → no se consideran campos variables de **cabecera IP** **TOS, TTL, flags, offset y checksum**



- Next Header : Identifica la carga transportada en el datagrama IP
- Payload Length: Tamaño de la cabecera AH
- SPI: Identificación de la Asociación de Seguridad (SA) utilizada
- Sequence Number: contador antireplay, se incrementa en cada envío
- Authentication Data: Contiene el ICV del datagrama

### funcionamiento AH:



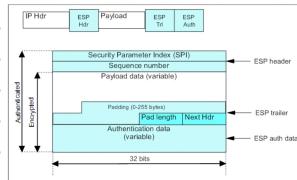
# T2 : IPSEC

## (IPSEC)

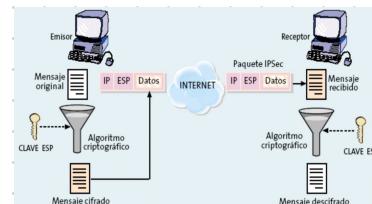
### Encapsulating Security Payload (ESP)

- Proporciona servicios
    - confidencialidad
    - autenticación del origen
    - integridad
    - anti replay
  - Next header = Protocolo = 50
  - Sobre datagramas no fragmentados
  - (si activa confidencialidad) → 1) comprueba integridad → 2) descifra
  - carga procesador enviar ataques Dos
- una vez aplicado ESP podrán ser fragmentados por los intermediarios

### Formato ESP



- Security Parameter Index (32 bits): Identificador de la SA
- Sequence Number (32 bits): Contador anti replay.
- Payload Data (variable): Datos de usuario cifrados con el algoritmo negociado en la Asociación de Seguridad (SA)
- Padding (0-255 bytes): Ajusta los datos al tamaño de bloque de cifrado y permite cuartelar la longitud de los datos originales
- Pad Length (8 bits): Tamaño del campo Padding
- Next Header (8 bits): Tipo de datos contenido por el datagrama
- Authentication Data: Control de integridad, similar al AH aunque no incluye la cabecera del datagrama IP



### Asociación de Seguridad (SA)

acuerdo entre 2 entidades IPsec sobre mecanismos seguridad a emplear

#### Para cada servicio utilizado (AH o ESP)

- se necesita un SA generar manualmente o automáticamente

puerto 500/udp protocolos ISAKMP/Oakley

- + **ISAKMP**: define entorno de gestión SA (negociación, modif., etc...)

[Internet Security Association & Key Management]

- + **Oakley**: especifica el modo seguro de intercambio → de una clave entre 2 partes, q no se conozcan

[Very Deterministic Protocol]

### Protocolo IKE (Internet Key Exchange)

- combinación ISAKMP/Oakley
- encarga establecimientos SAs → distrib. de claves
- ofrece + métodos de autenticación
  - Clave Compartida
  - Firmas Digitales (requiere certificados)
  - Reto-Respuesta con claves Públicas/priv

### Fases IKE

#### Fase 1

- establece secreto del cual derivan las claves
- Criptografía asimétrica: para establecer:
  - SA de IKE entre extremos
  - claves q → IKE
- Finaliza: → Fase 2

#### Fase 2

- se negocian SA + sus claves
- se actualizan periódicamente

## Túneles

transfieren **IP** de datos de un protocolo encapsulado dentro del **IP** de datos de otro protocolo (o del mismo)

- Túnel proporciona capacidad de enrutamiento a IP → direcciones ilegales q no deben moverse directamente por la red
- Túnel q no deben moverse directamente por la red
- Juntas no son rutas
- ...

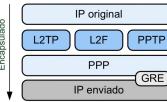
• Destino: IP original no desempaquetado (routa original)

- Túnel → no proporciona seguridad → no es una tecnología novedosa ej: IP sobre Frame Relay
- Soluciones túneles con seguridad: PPTP, L2TP, IPsec, ...

### Tipos de túneles

- Túneles Nivel 2: FR, ATM o PPP

- Túneles Nivel 3: Encapsulado directo sobre IP



Túnel de nivel 2



Túnel de nivel 3

### Secuencia de intercambio:

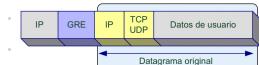


### GRE (Generic Routing Encapsulation)

protocolo de túneles para el encapsulamiento de una gran variedad de protocolos red (IP, IPX, AppleTalk) sobre IP

simulando enlaces virtuales punto a punto  
no incluye cifrado

- de la opción, una subcabeza GRE (protocolo=47) y se encapsula → datagrama IP



interface tunnel<num>

tunnel source <interface>  
tunnel destination <ip\_addr>  
tunnel mode gre | ipv6ip | ...  
ip address ...

### Ejemplo de túnel Nivel 3: IPsec

- datagramas origen son encapsulados dentro datagrama → intercambio metadatos
- Caso: ESP en modo túnel → proporciona confidencialidad, integridad



### Configuración de un túnel GRE + IPsec

```
crypto isakmp policy 15
encr 3des
hash md5
authentication pre-share
group 2
crypto isakmp key <mi_clave> address 192.168.0.2 255.255.255.252
crypto ipsec profile ipsecprof
set transform-set myself
interface Tunnel0
  tunnel source Serial0
  tunnel destination 192.168.0.2
  tunnel protection ipsec profile ipsecprof
```