Módulo V
Acceso Remoto
y
Redes Privadas Virtuales

Programa

1. ***Seguridad en comunicaciones.***
2. ***Protocolos de seguridad de capa de aplicación. (SSH)***
3. ***Protocolos de seguridad de capa de transporte. (SSL/TLS)***
4. ***Seguridad en redes inalámbricas.***
5. ***Protocolos de seguridad de la capa de enlace.***
6. ***Protocolos de seguridad de la capa de red. (IPSec)***
7. ***Redes privadas virtuales.***
8. ***Implementación de redes privadas virtuales.***

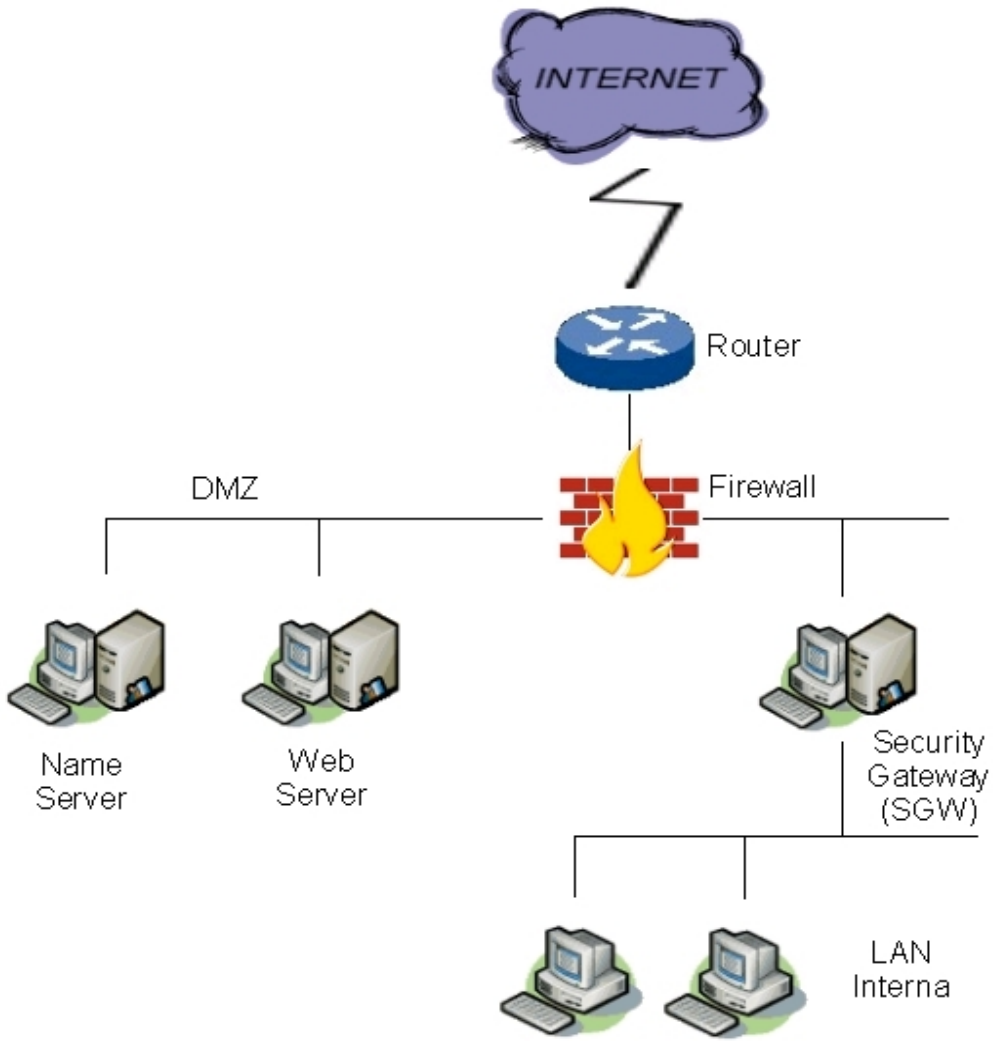
Seguridad en Comunicaciones

- ***Vulnerabilidades de protocolos actuales:***
  - ***Basados en contraseñas***
  - ***Información en texto plano***
  - ***No hay mecanismos de autenticación***
  - ***No hay mecanismos de verificación de integridad***
  - ***Susceptibilidad a sobreflujo de buffers***
  - ***Ejemplos: FTP, Telnet, SMTP, POP, IMAP, etc.***

Amenazas

- ***Intercepción de información***
  - ***Sniffing***
  - ***Eavesdropping***
- ***Suplantación de usuarios legítimos***
  - ***Ataques de diccionario sobre contraseñas***
  - ***Ataques en línea***
  - ***Session hijacking***
- ***Inyección de paquetes***
- ***Análisis de tráfico***
- ***Denegación de servicios***

Acceso Remoto



Secure Shell – SSH

- **SSH es un protocolo de acceso remoto seguro a través de redes inseguras.**
- **Consiste de tres componentes:**
  - ***Protocolo de capa de transporte (SSH-TRANS)***
    - **Autenticación,confidencialidad, integridad y, opcionalmente, compresión.**
    - **Usualmente sobre TCP**
  - ***Protocolo de autenticación de usuario (SSH-USERAUTH)***
    - **Autentica clientes.**
  - ***Protocolo de conexión (SSH-CONNECT)***
    - **Multiplexa paquetes cifrados por túneles diferentes.**

SSH – Arquitectura

- **Claves de host**
  - **Cada servidor debe poseer al menos una clave.**
  - **El cliente debe conocer previamente clave pública del host.**
- **Modelos de confianza:**
  - **Base de datos local al cliente con claves públicas.**
  - **Certificados digitales (PKI).**

SSH – Transporte

- **Cifrado de datos:**
  - **Cifrado simétrico: 3DES, Blowfish, Twofish, AES, Serpent, Arcfour, IDEA, Cast, None.**
  - **Todos en modo CBC.**
- **Integridad de datos:**
  - **Algoritmos MAC: HMAC-SHA1, HMAC-MD5, None.**
- **Intercambio de claves: Diffie-Hellman.**
- **Algoritmos de clave pública:**
  - **DSS, RSA, Certificados X509v3, Certificados SPKI, Certificados OpenPGP**

SSH – Autenticación

- **Autenticación por clave pública.**
  - **El usuario envía, firmado con su clave privada:**
    - **Identificador de sesión**
    - **SSH_MSG_USERAUTH_REQUEST**
    - **Nombre de usuario**
    - **Servicio**
    - **“public key”**
    - **TRUE**
    - **Nombre del algoritmo de clave pública**
    - **Clave pública a utilizar**
  - **El servidor verifica la firma digital.**

SSH – Autenticación

- **Autenticación por contraseña.**
  - **El usuario envía la petición:**
    - **SSH_MSG_USERAUTH_REQUEST**
    - **Nombre de usuario**
    - **Servicio**
    - **“password”**
    - **FALSE**
    - **Contraseña en texto plano**
  - **El servidor verifica la contraseña del usuario.**
  - **El servidor responde con éxito o falla.**

SSH – Autenticación

- **Autenticación basada en host.**
  - **El usuario envía la petición:**
    - **SSH_MSG_USERAUTH_REQUEST**
    - **Nombre de usuario**
    - **Servicio**
    - **“hostbased”**
    - **Algoritmo de clave pública para el host**
    - **Clave pública de host (certificado de host)**
    - **Nombre de host cliente**
    - **Nombre de usuario del host cliente**
    - **Firma digital**
  - **El servidor verifica clave del host, los permisos del usuario y la validez de la firma digital.**

SSH – Conexión

- **Mecanismo de canal.**
  - **Canal: Sesiones de terminal, conexiones redirigidas, etc.**
  - **Canales múltiples son multiplexados a través de una sola conexión.**
  - **Los canales son identificados por un número en cada lado.**
- **Apertura de canal:**
  - **Mensaje de apertura de canal:**
    - **Tipos de canal: session, x11-req, tcpip-forward, env, shell, exec, signals.**

Seguridad de SSH

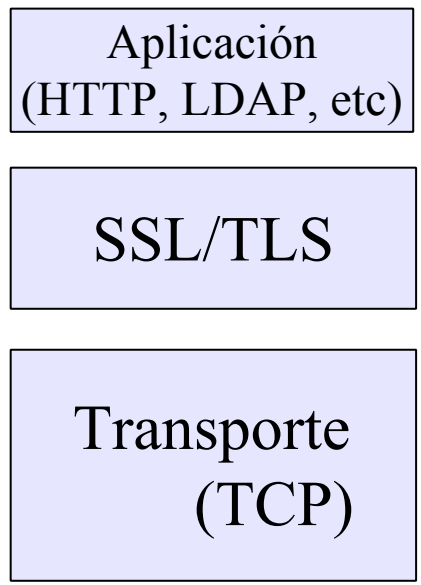
- **Generación de números seudoaleatorios.**
- **Transporte:**
  - **Ataque de hombre en medio.**
  - **Denegación de servicio (*"wire cutter"*).**
  - **Canal secreto (*"covert channel"*).**
- **Autenticación**
  - **Autenticación por clave pública: Compromiso de cliente.**
  - **Autenticación por contraseña: Compromiso de servidor.**
  - **Autenticación basada en host: Compromiso de cliente.**

Implementaciones de SSH

- **SSH Communications Security: http://www.ssh.com/**
- **OpenSSH: http://www.openssh.com/**
- **LSH: http://www.lysator.liu.se/~nisse/lsh/**
- **F-Secure SSH: http://www.f-secure.com/**
- **PuTTY: http://www.chiark.greenend.org.uk/~sgtatham/putty/**
- **VshelI (SSH-2 server Win): http://www.vandyke.com/products/vshell/**
- **TeraTerm: http://www.zipworld.com.au/~roca/ttssh.html**
- **MindTerm (Java): http://www.mindbright.se/mindterm/**

SSL/TLS

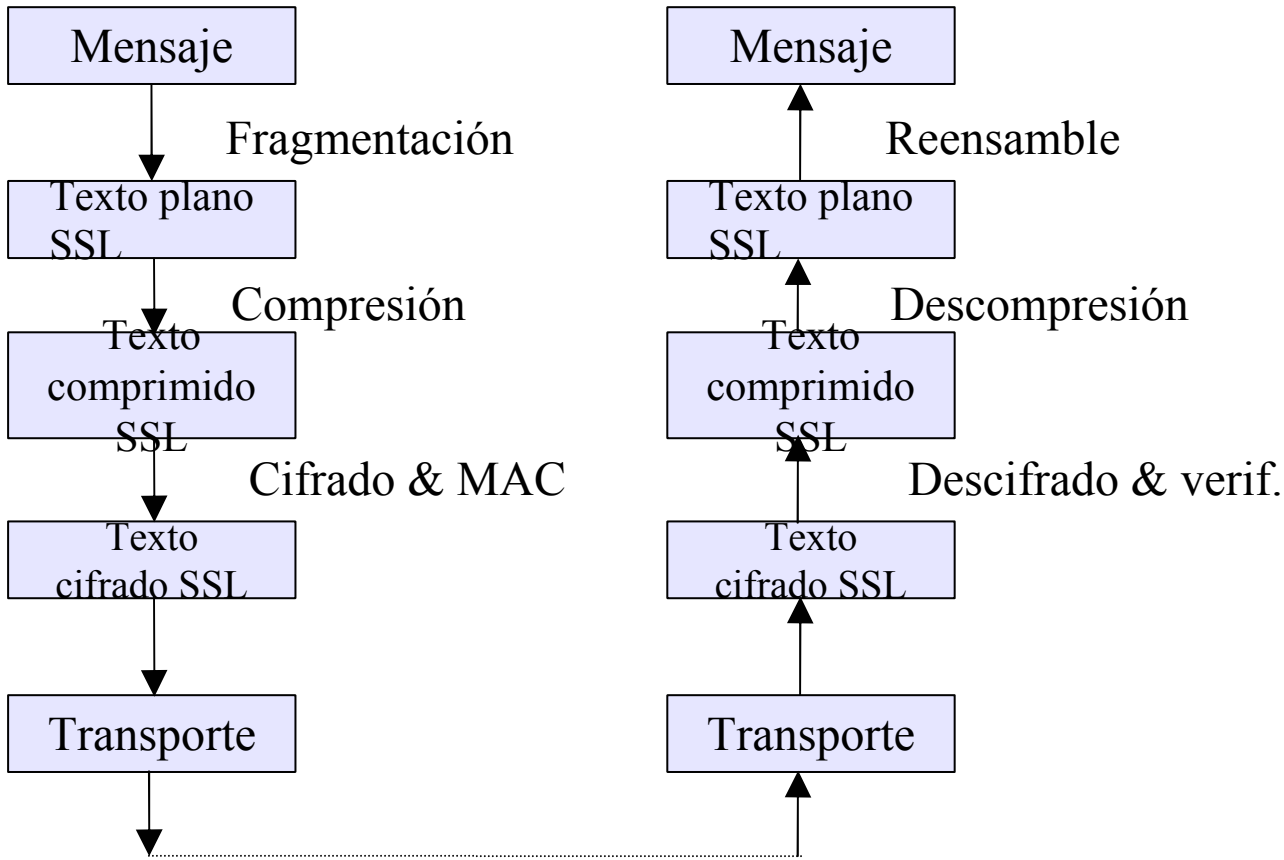
- **SSL (Secure Socket Layer) – Diseñado por Netscape.**
- **TLS (Transport Layer Security) – Estándar de IETF.**
- **Proporciona:**
  - **Cifrado de datos**
  - **Autenticación de servidor**
  - **Integridad de mensajes**
  - **Autenticación de cliente (op)**
- **Compuesto de dos protocolos**
  - ***SSL Record***
  - ***SSL Handshake***



SSL Record Protocol

- **Utilizado para el encapsulamiento de protocolos de nivel superior.**
- **Recibe datos de capas superiores y los transfiere a texto cifrado de SSL.**
- **Recibe datos cifrados de capas inferiores y transfiere a datos originales**
  - **Fragmentar/ Reensamblar**
  - **Comprimir / Descomprimir**
  - **Cálculo de MAC / Verificación de MAC**
  - **Cifrado / Descifrado**

SSL Record Protocol



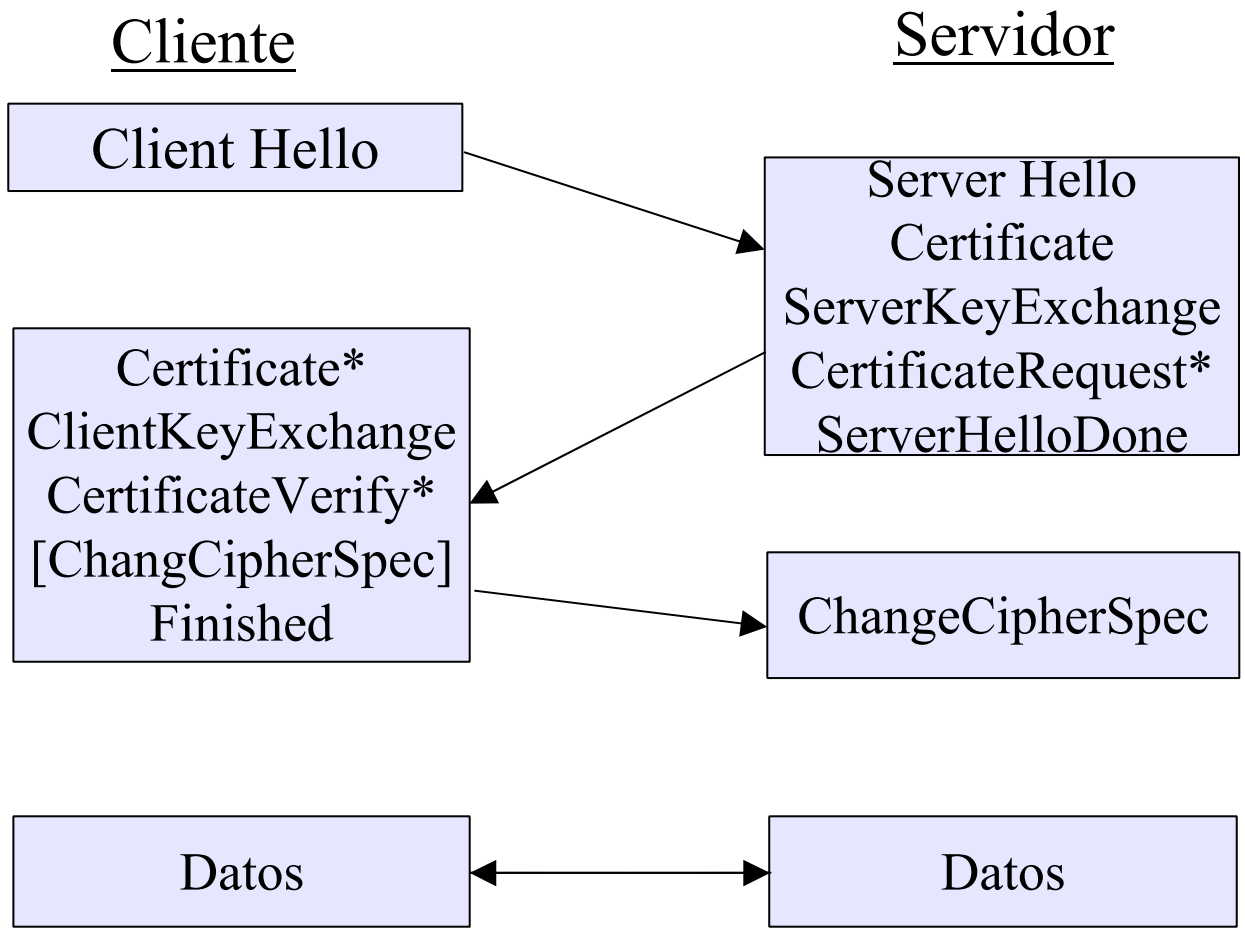
SSL Handshake Protocol

- **Utilizado para la negociación de los atributos de seguridad de una sesión entre cliente y servidor.**
- **Funciona sobre la capa de registro de SSL**
  - **Acuerda versión del protocolo**
  - **Selecciona algoritmos criptográficos**
  - **Realiza autenticación mutua**
  - **Genera clave de sesión**

SSL Handshake Protocol

- **Establecimiento de Sesión:**
  - **Identificador de sesión**
  - **Certificados de las partes**
  - **Método de compresión**
  - **Especificación de cifrado**
    - **Algoritmo de cifrado (DES, 3DES, RC2, RC4, IDEA, Fortezza, NULL)**
    - **Algoritmo MAC (MD5, SHA1, Null)**
  - **Secret master**
  - **Resumable**

SSL Handshake Protocol



Seguridad en Redes Inalámbricas

- ***La seguridad en redes inalámbricas y en dispositivos móbiles es difícil de lograr debido a varias restricciones:***
  - ***Los protocolos deben tolerar amplios tiempos de retardo en las comunicaciones.***
  - ***Los anchos de banda de algunas portadoras son muy bajos.***
  - ***El poder de procesamiento de muchos dispositivos es muy limitado.***
  - ***La capacidad de memoria es muy limitada en la mayoria de los dispositivos.***
  - ***Se tienen restricciones en la exportación y utilización de criptografía.***

IEEE 802.11b

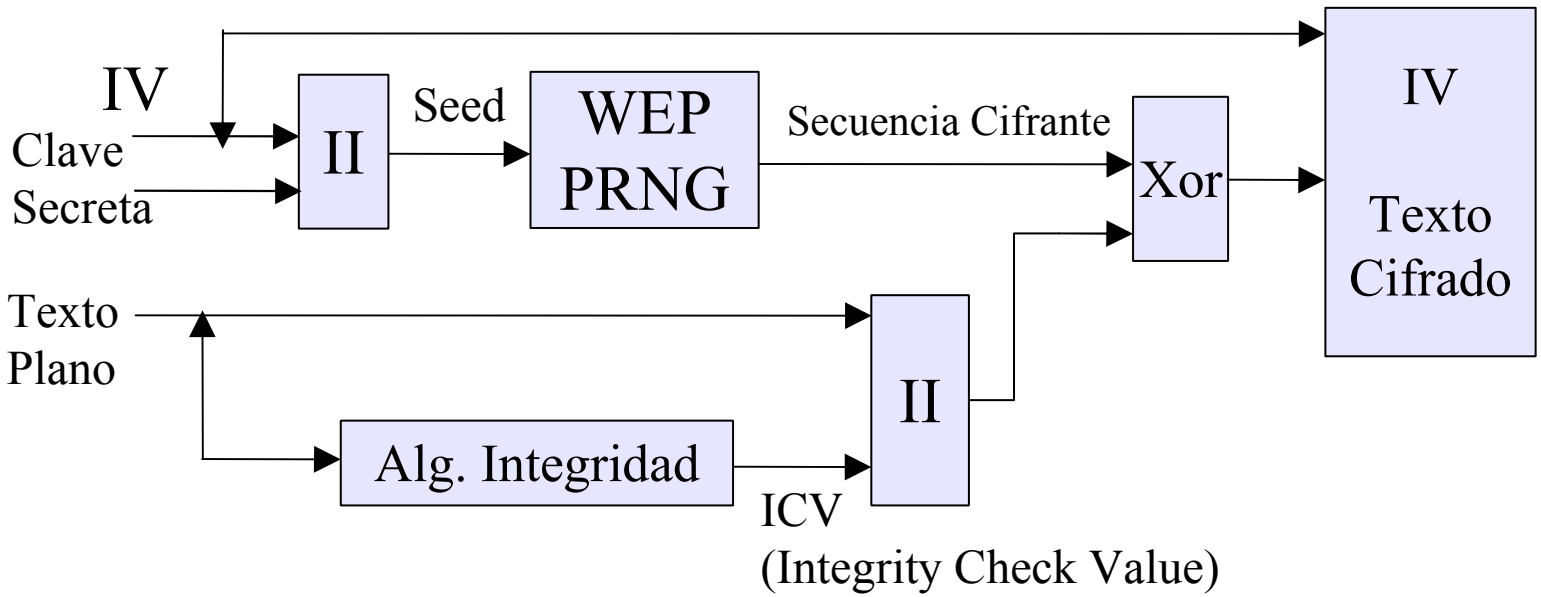
- ***Características:***
  - ***Velocidad: 11 Mbps***
  - ***Uso: LAN de oficina***
  - ***Tipo de terminales: Laptops, desktops, handhelds, gateways.***
  - ***Configuración típica: Múltiples clientes por punto de acceso.***
  - ***Rango: Entre 15 y 100 metros.***
  - ***Tecnología de comunicación: Expansión de espectro por secuencia directa.***

IEEE 802.11b – Autenticación

- ***Open System authentication:***
  - ***Algoritmo de autenticación nulo.***
  - ***Cualquier STA que solicite autenticación es aceptada.***
- ***Shared Key authentication:***
  - ***Autentica a las STA que poseen una clave secreta compartida.***
  - ***Solo si está habilitado WEP.***
  - ***Durante la autenticación, se transmiten tanto el reto como el reto cifrado (!!)***

WEP – Wired Equivalent Privacy

- ***El objetivo de WEP es proporcionar confidencialidad de datos en una WLAN IEEE 802.11***



Características de WEP

- ***El vector de inicialización (IV) es de 3 bytes (24 bits).***
- ***Se puede reutilizar IV.***
- ***La clave secreta es de 5 bytes (40 bits). Susceptible a ataque por fuerza bruta.***
- ***La clave secreta usualmente es compartida por varias STA.***
- ***El algoritmo generador de la secuencia cifrante es RC4.***
- ***El ICV (Integrity Check Value) es de 32 bits.***
- ***El algoritmo utilizado para verificación de integridad es CRC-32.***

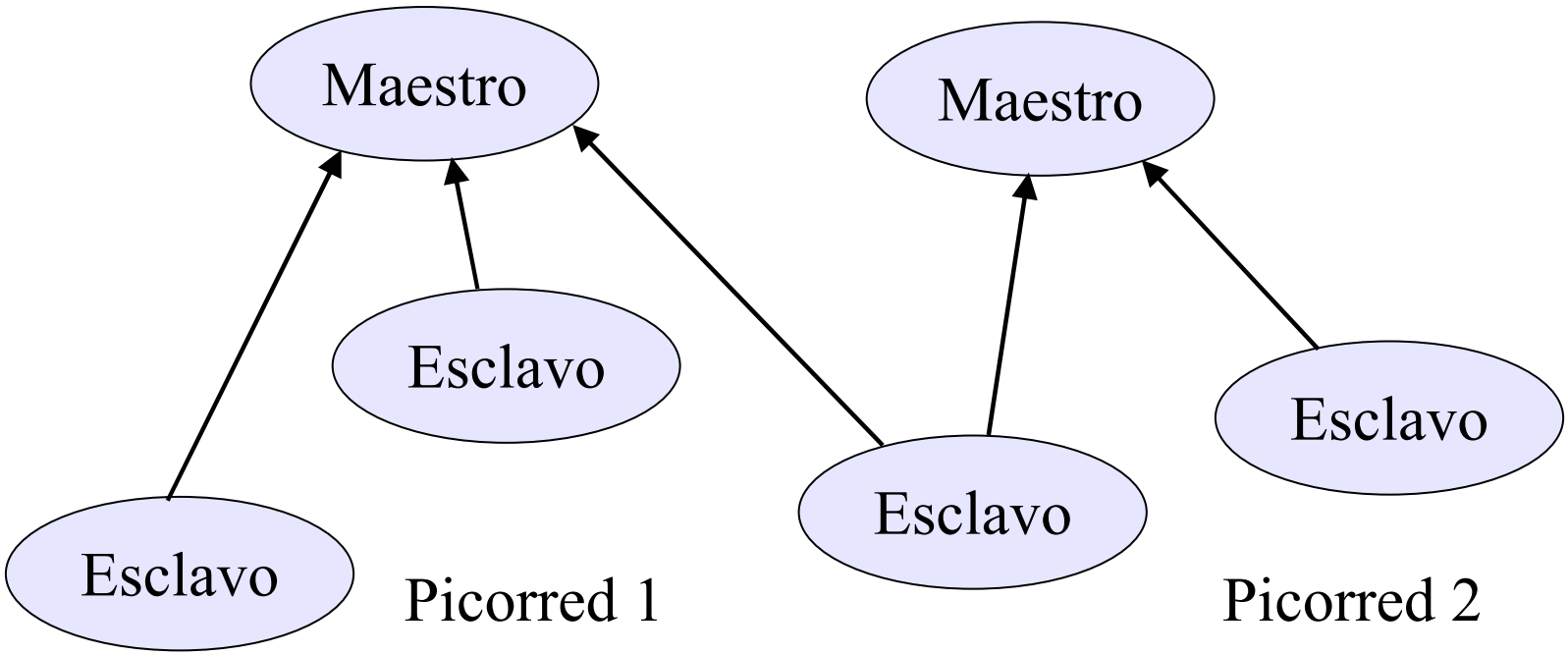
(In)Seguridad de WEP

- ***Susceptible a múltiples ataques:***
  - ***Reuso de IV***
  - ***Ataque de texto plano conocido***
  - ***Ataque de texto plano parcial***
  - ***Ataque de fuerza bruta sobre la clave***
  - ***Descifrado en tiempo real (mediante diccionarios de IV y claves)***
- ***Software:***
  - ***http://airsnort.sourceforge.net/***
  - ***http://sourceforge.net/projects/wepcrack/***

Bluetooth

- ***Características:***
  - ***Velocidad: 30-400 Kbps***
  - ***Uso: Redes de área personal (PAN o picorredes)***
  - ***Tipo de terminales: Laptops, celulares, handhelds, localizadores, electrodomésticos y coches.***
  - ***Configuración típica: Punto a punto o múltiples dispositivos por punto de acceso.***
  - ***Rango: 10 metros.***
  - ***Tecnología de comunicación: Salto de frecuencia de banda estrecha.***

Redes Dispersas



Seguridad de Bluetooth

- ***Modos de seguridad:***
  - ***Modo 1 – Sin seguridad.***
  - ***Modo 2 – Modo de seguridad a nivel de servicio. No se realiza autenticación, ni cifrado antes del establecimiento del canal.***
  - ***Modo 3 – Modo de seguridad a nivel de enlace. Se inician procedimientos de seguridad antes del establecimiento del canal.***
- ***Cada dispositivo cuenta con una dirección publica única (BD_ADDR).***

Seguridad de Bluetooth

- ***Manejo de claves:***
  - ***Clave de enlace (128 bits):***
    - ***Utilizada durante la autenticación***
    - ***Parámetro para derivación de clave de cifrado.***
    - ***Pueden ser:***
      - ***Clave de unidad***
      - ***Clave de combinación***
      - ***Claves de inicialización***

Seguridad de Bluetooth

- ***Manejo de claves:***
  - ***Clave de unidad (128 bits):***
    - ***Generada cuando un dispositivo es utilizado por vez primera.***
    - ***Generada mediante algoritmo E21, utilizando un número aleatorio de 128 bits y la dirección del dispositivo.***
    - ***Almacenada en memoria no-volatil.***
  - ***Clave de inicialización (128 bits):***
    - ***Generada cuando dos dispositivos se comunican por vez primera.***
    - ***Generada mediante E22 a partir de un random de 128 bits y un NIP de 4 dígitos.***

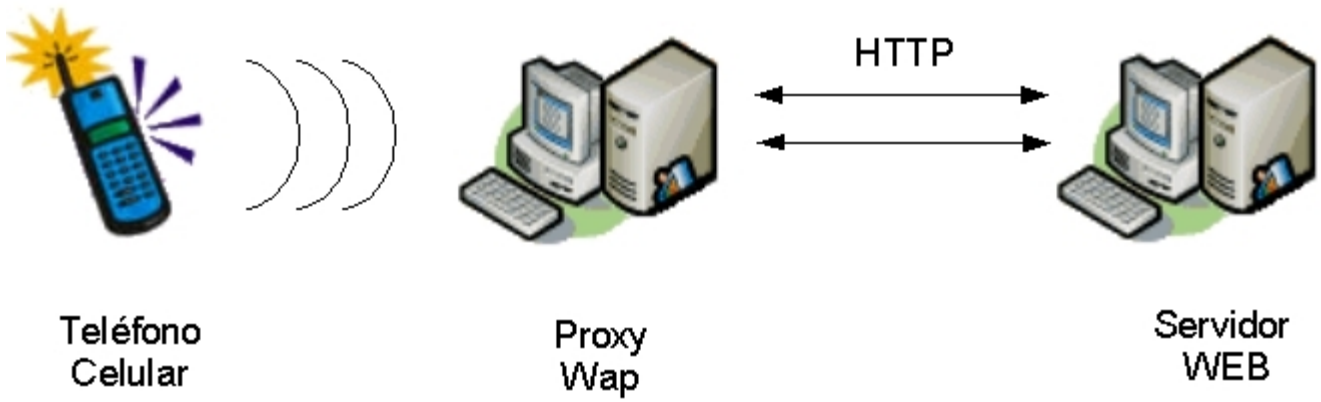
Seguridad de Bluetooth

- ***Cifrado:***
  - ***Mediante algoritmo de cifrado en flujo E0, que utiliza cuatro registros LFSR de longitudes 25, 31, 33 y 39.***
  - ***El valor inicial de los registros LFSR es derivado de la clave de cifrado.***
- ***Autenticación:***
  - ***Mediante un protocolo de reto respuesta.***
  - ***Verifica que ambos dispositivos compartan la misma clave de enlace.***
- ***Análisis de seguridad de Bluetooth:http://www.niksula.cs.hut.fi/~jiitv/bluesec.html***

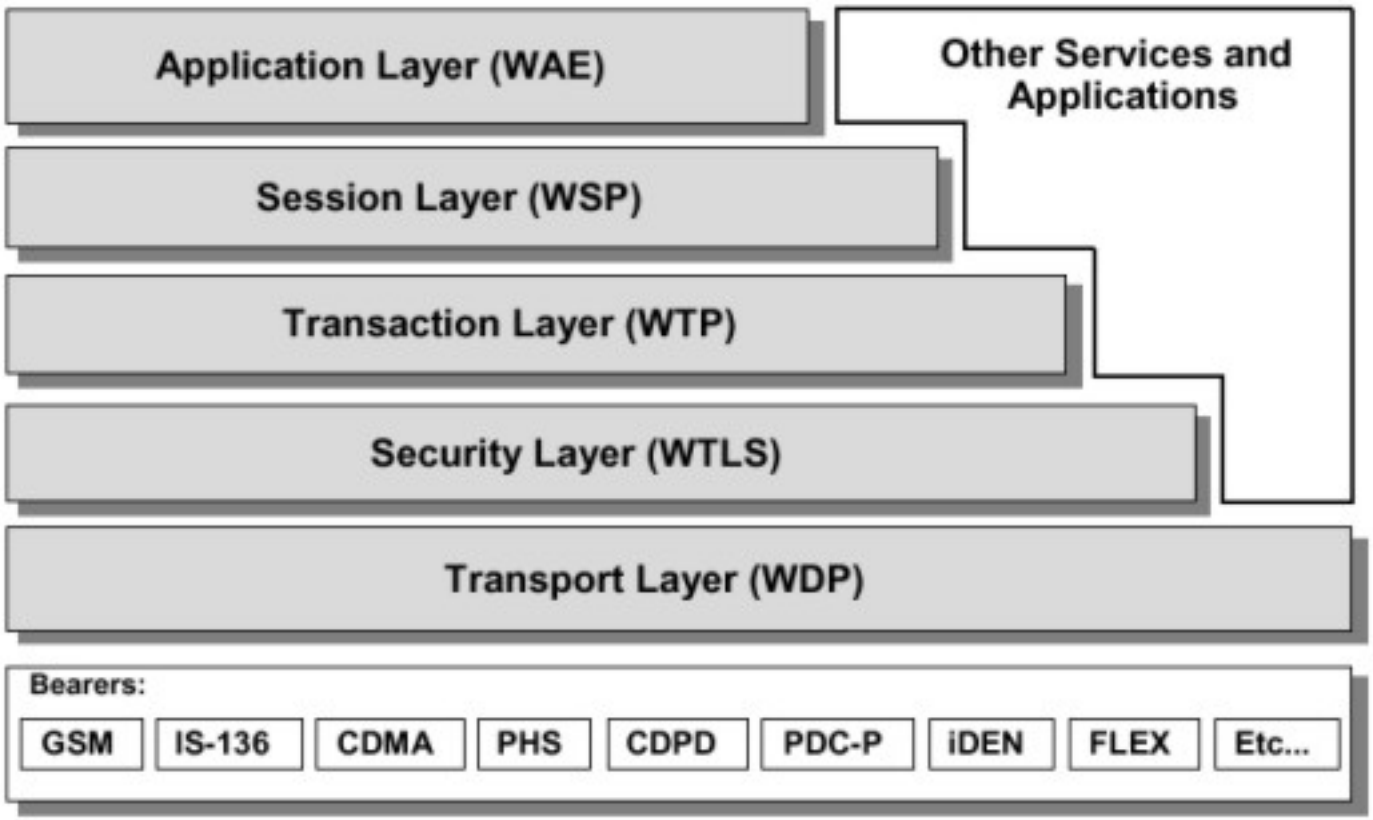
WAP – Wireless Application Protocol

- ***El protocolo WAP es el estándar principal para servicios de información para dispositivos inalámbricos.***
- ***Está basado en estándares de Internet (XML, TCP/IP).***
- ***Consiste en una especificación del lenguaje WML, una especificación de WMLScript, y una especificación de la WTAI (Wireless Telephony Application Interface).***
- ***Es un protocolo diseñado para micro-browsers.***
- ***Utilizado en dispositivos handheld tales como teléfonos celulares, pagers, palmtops, etc.***
- ***Implementado sobre PalmOS, Windows CE, FLEXOS, OS/9, JavaOS, etc.***

Proxy WAP

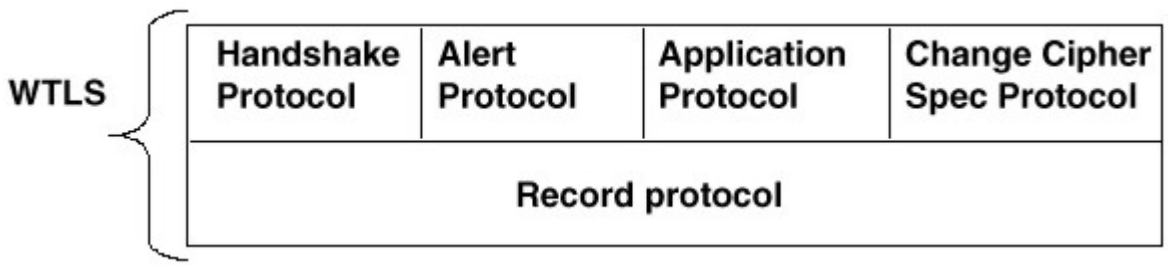


Pila de protocolos WAP

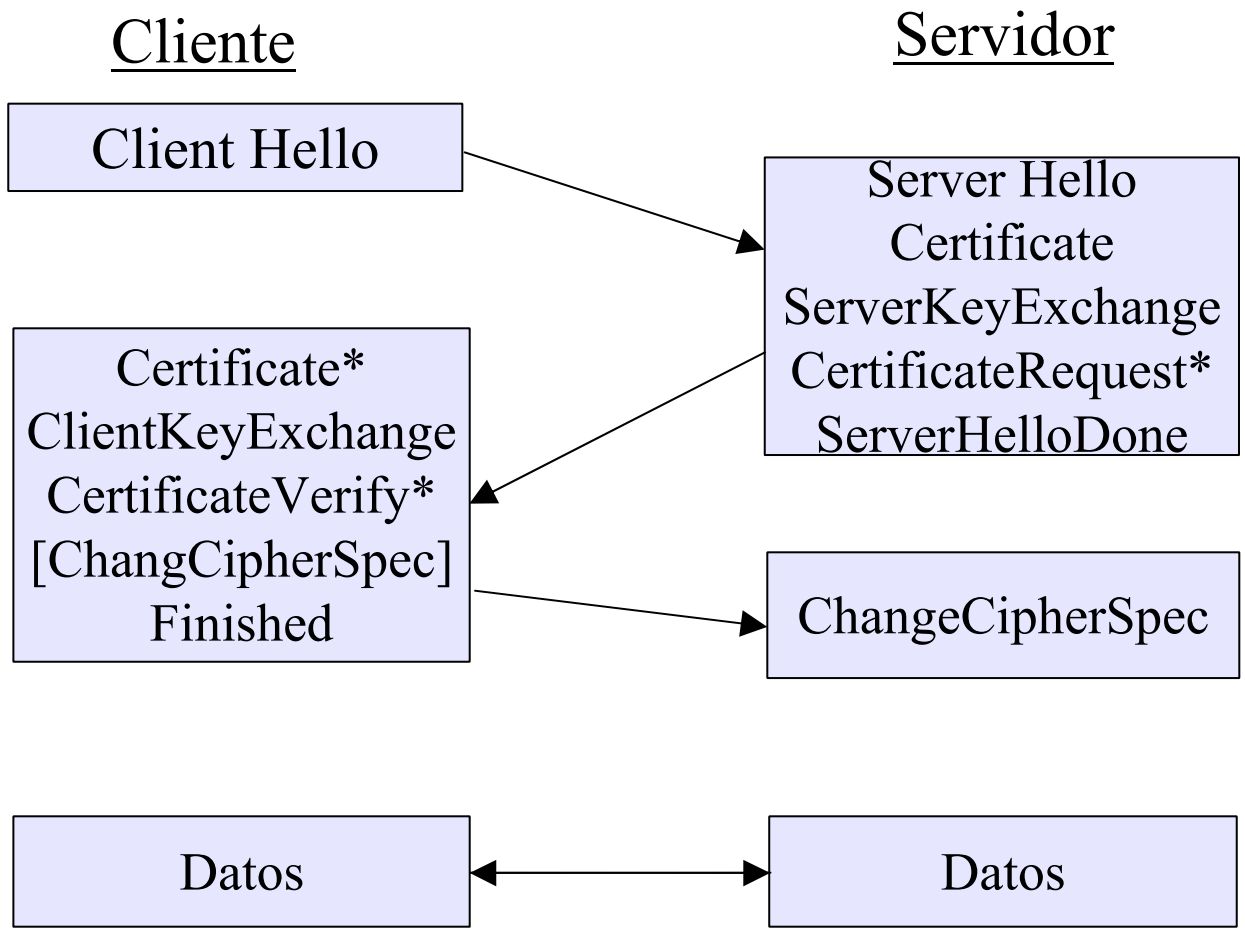


WTLS – Wireless TLS

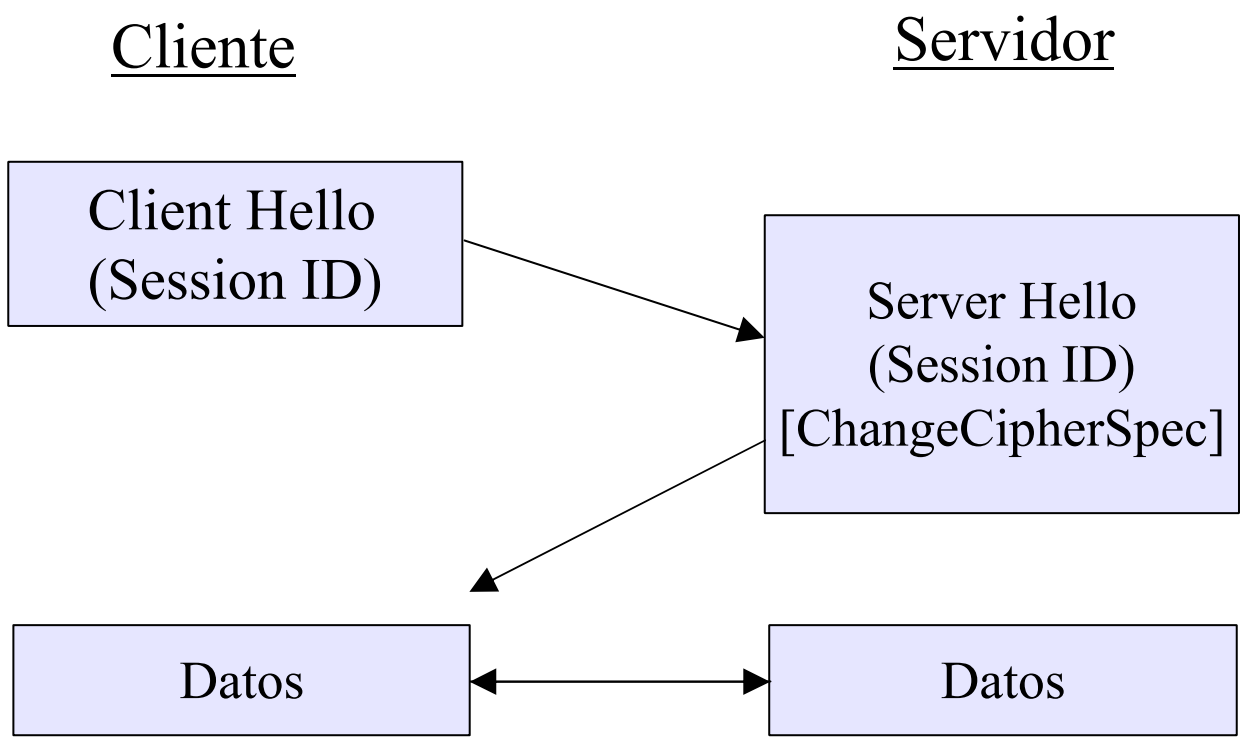
- ***WTLS (Wireless Transport Layer Security) es la capa de seguridad para el protocolo WAP.***
- ***WTLS está basado en TLS v1, con modificaciones para un entorno inalámbrico:***
  - ***Soporte para datagramas.***
  - ***Tamaño de paquete optimizado.***
  - ***Uso de algoritmos criptográficos rápidos.***



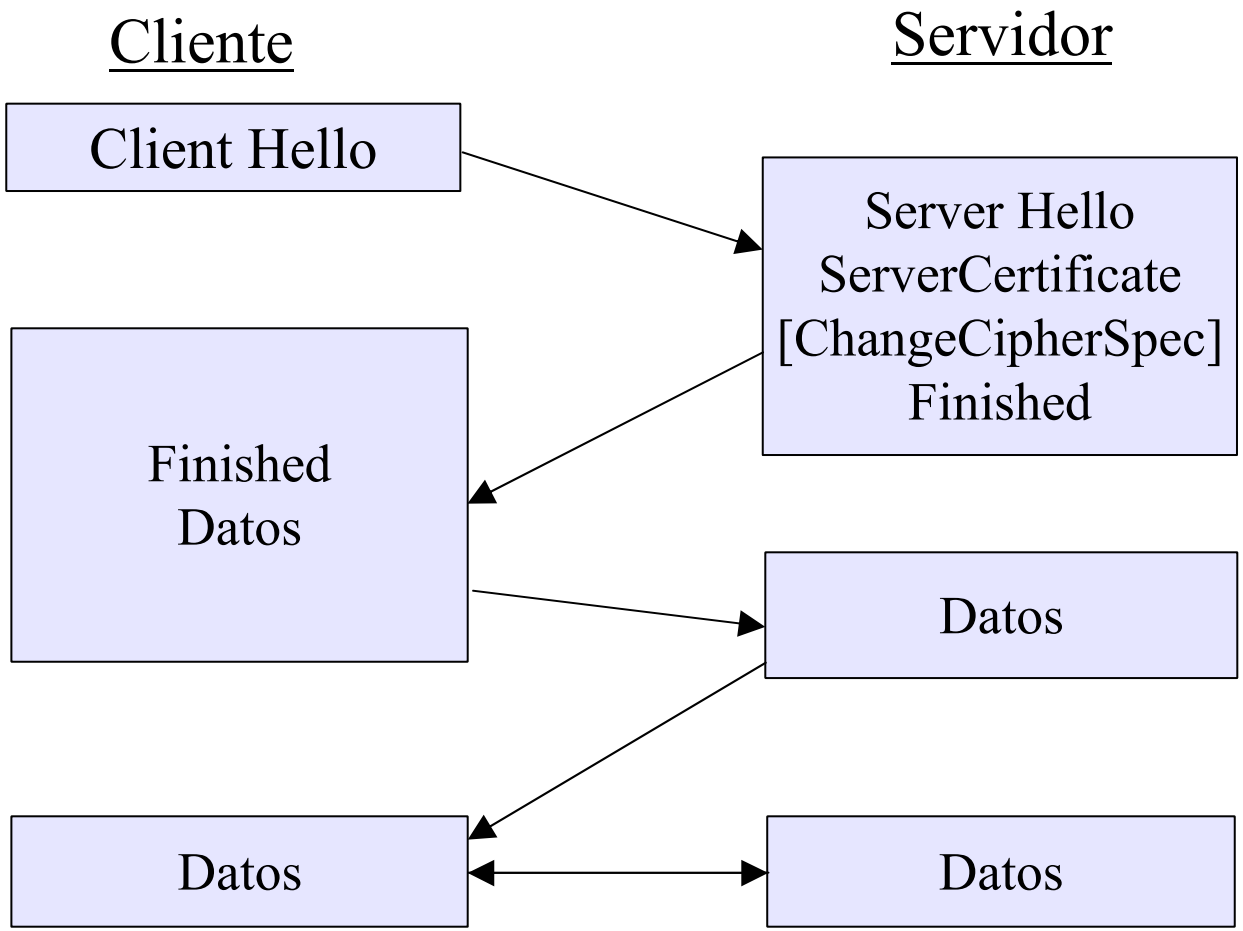
WTLS Handshake Protocol



Resumed Handshake



Optimized Handshake



Autenticación en WTLS

- ***Autenticación mediante certificados:***
  - ***Autenticación mutua o solo del servidor.***
  - ***Soporta certificados X.509v3, X9.68 y certificados WTLS.***
- ***Intercambio de claves (no certificadas)***
  - ***RSA, DH, ECDH.***
- ***Suites de cifrado***
  - ***RC5 con claves de 40, 56 y 128 bits.***
  - ***DES con claves de 40 y 56 bits.***
  - ***3DES e IDEA con claves de 40, 56 y 128 bits.***
  - ***NULL***
- ***Verificación de integridad: SHA, MD5, XOR-40***

(In)Seguridad en WTLS

- ***IV predecibles y ataques de texto plano escogido.***
- ***XOR MAC no proporciona suficiente protección de la integridad de los mensajes.***
- ***Cifrado DES de 35 bits:***
  - ***Claves DES de 40 bits, 1 bit de paridad por byte.***
  - ***5*7=35 bits efectivos.***
  - ***Susceptible a ataque por fuerza bruta.***
- ***Mensajes de alerta no autenticados***
- ***Fugas de información en texto plano (IV inicial, cambio de especificaciones de cifrado)***

Otros protocolos inalámbricos

- ***HomeRF (http://www.homerf.org)***
  - ***Opera también en el espectro de 2.4GHz.***
  - ***Velocidades de 1.6 Mbps.***
  - ***Utiliza cifrado de 56 bits (no exportable).***
  - ***Autenticación mediante contraseña.***
- ***IrDA – Infrared Data Association***
  - ***No implementa ningún mecanismo de seguridad, se deja a la aplicación.***

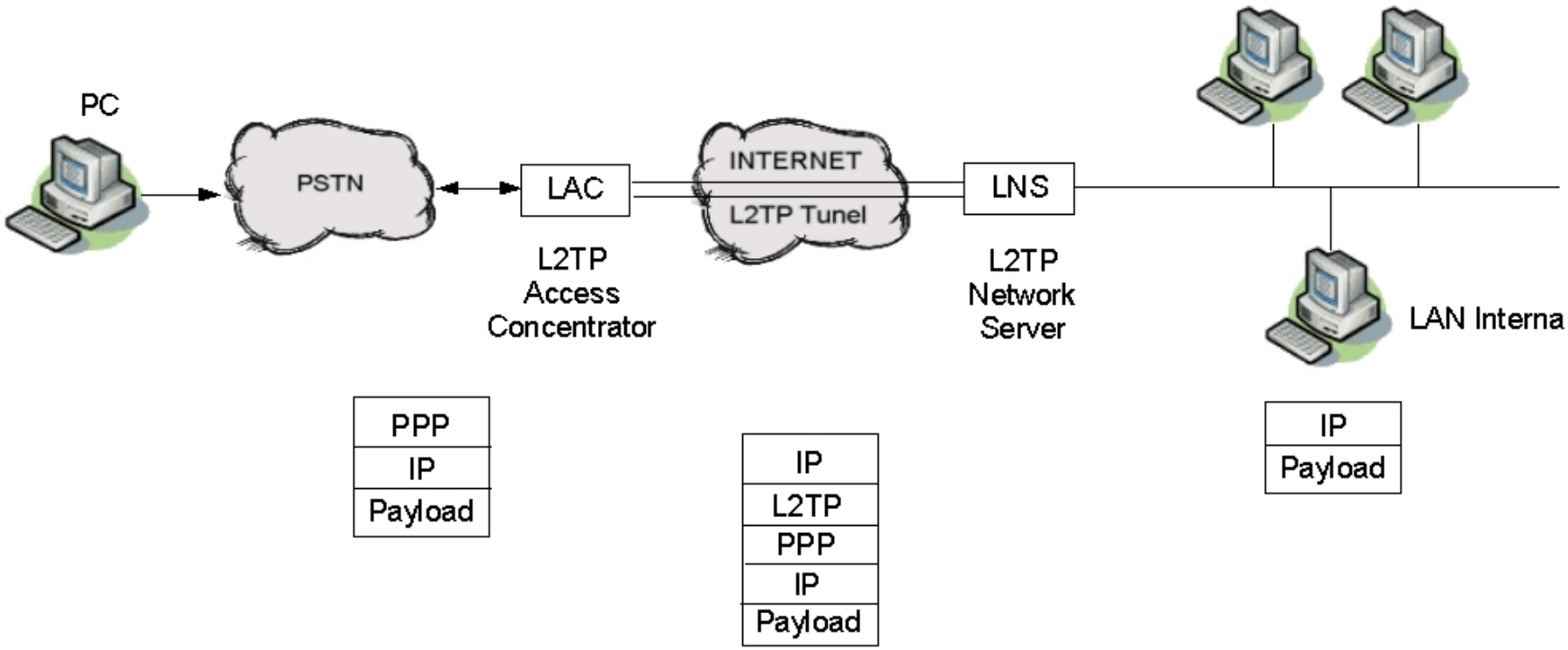
Protocolos de Seguridad de la Capa de Enlace

- ***PPTP – Point-to-Point Tunneling Protocol***
  - ***Creado por el PPTP Forum (Microsoft, et. al.)***
  - ***Actualmente es considerado inseguro, ha sido reemplazado en W2k por IPSec.***
- ***L2TP – Layer 2 Tunneling Protocol***
  - ***Ver: RFC 2661, 2888.***
  - ***Usualmente se utiliza en combinación con IPSec***
- ***L2F – Layer 2 Forwarding***
  - ***Diseñado por Cisco***
  - ***Ver: RFC 2341***
  - ***Al igual que L2F permite un dial up virtual.***
  - ***Por tanto debe utilizarse en combinación con IPSec.***

(In)Seguridad de PPTP

- ***Autenticación: Microsoft Challenge/Reply Handshake Protocol (MS-CHAP)***
- ***Cifrado: Microsoft Point to Point Encryption (MS-PPE)***
- ***MS-PPE fue criptoanalizado en 1998: El cifrado puede anularse haciendo XOR de dos mensajes.***
- ***MS-CHAPv1***
  - ***Uso de LANM hash. (Rompibles con L0phtcrack)***
  - ***El servidor puede ser suplantado.***
  - ***DoS mediante spoofing de paquetes de falla MS-CHAP.***
- ***MS-CHAPv2 no mejoró la seguridad significativamente.***
- ***Ver detalles en: http://www.schneier.com/paper-pptpv2.html***

L2TP


PC
PSTN
LAC
INTERNET
L2TP Tunel
LNS
L2TP
Access
Concentrator
L2TP
Network
Server
LAN Interna
PPP
IP
Payload
IP
L2TP
PPP
IP
Payload
IP
Payload

IPSec

- *IPSec proporciona servicios de seguridad en la capa IP.*
- *Permite:*
  - *Seleccionar los protocolos de seguridad requeridos.*
  - *Determinar los algoritmos a utilizar*
  - *Utilizar las claves criptográficas requeridas*
- *Utilizado para proteger uno o más "caminos" entre:*
  - *Un par de hosts*
  - *Un par de gateways de seguridad*
  - *Un gateway de seguridad y un host*

Protocolos IPSec

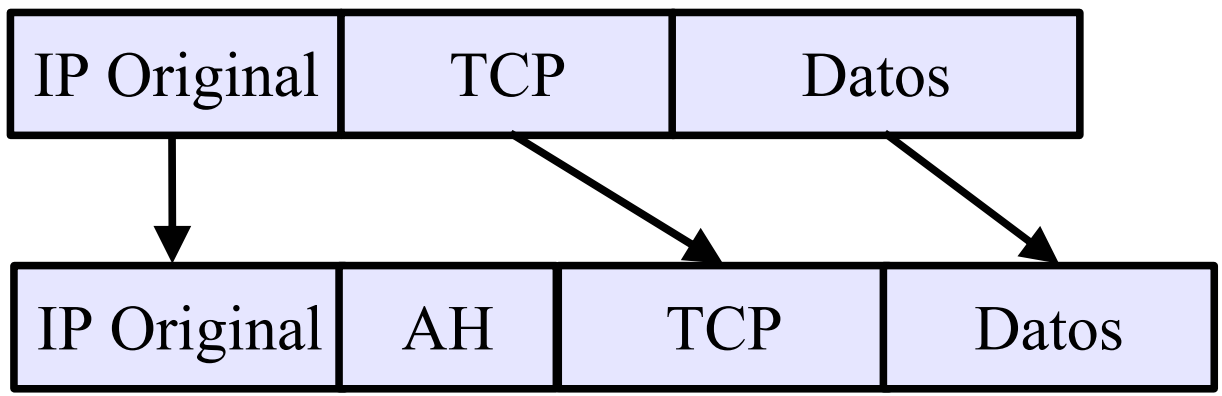
- ***IPSec utiliza dos protocolos:***
  - ***Authentication Header (AH) – Proporciona integridad de datos y autenticación de origen.***
  - ***Encapsulating Security Payload (ESP) – Proporciona confidencialidad, integridad de datos y autenticación de origen.***
  - ***Tanto AH y ESP implementan control de acceso mediante la distribución de claves públicas.***
  - ***Cada protocolo soporta dos modos:***
    - ***Modo de transporte***
    - ***Modo de túnel***

Security Associations

- ***Security Association (SA) – Es una "conexión" simplex que proporciona servicios de seguridad al tráfico que porta.***
- ***Pueden utilizar AH o ESP pero no ambos.***
- ***Para asegurar tráfico bidireccional entre dos host, o entre dos gateways de seguridad, se requieren dos SA.***
- ***Una SA es identificada de forma única por:***
  - ***Security Parameter Index (SPI)***
  - ***Dirección IP de destino***
  - ***Identificador de protocolo de seguridad (AH o ESP)***

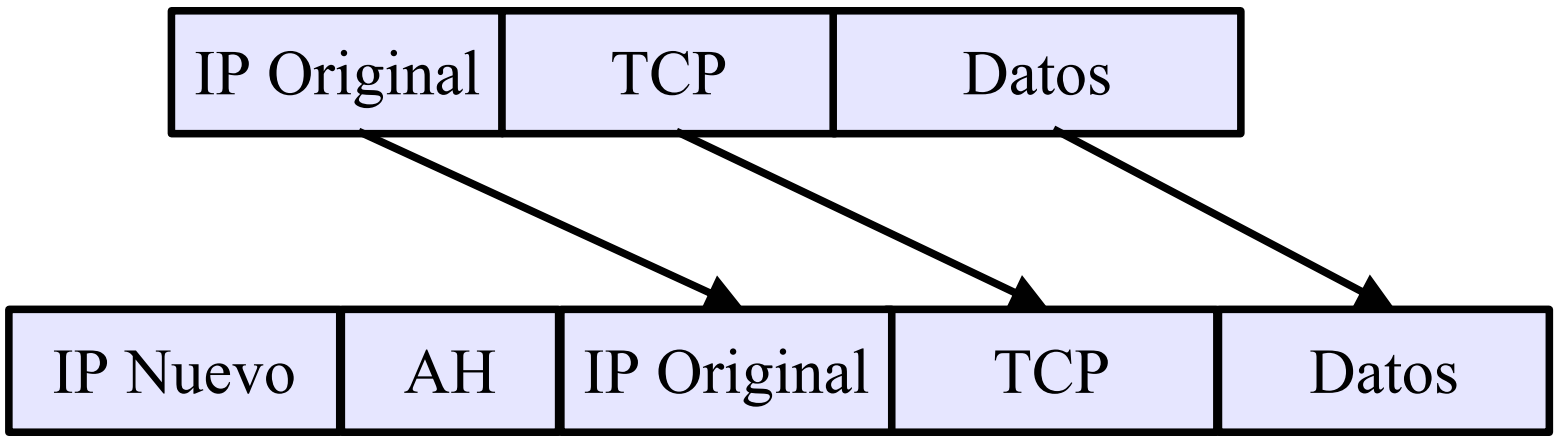
IP Authentication Header

- ***Authentication Header (AH) – Proporciona integridad y autenticación de origen.***
- ***Integridad y autenticación de los datos de aplicación.***
- ***Integración y autenticación a parte del encabezado IP.***
- ***Modo de transporte:***

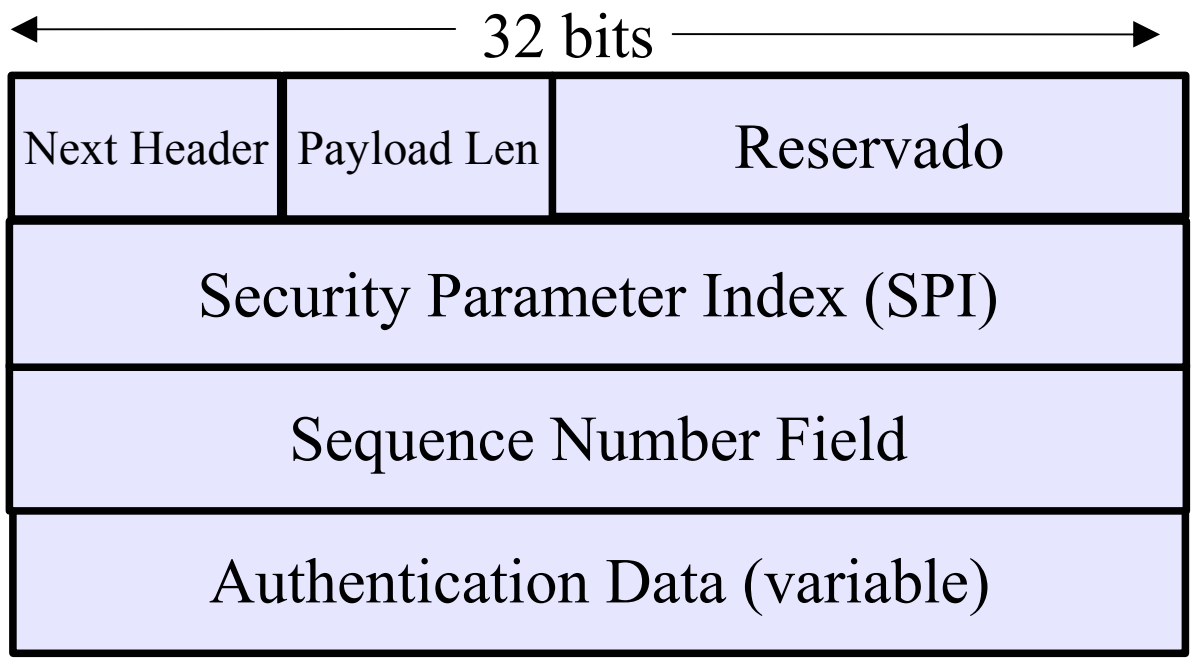


IP Authentication Header

- ***Modo de túnel:***



Encabezado AH



Encabezado AH

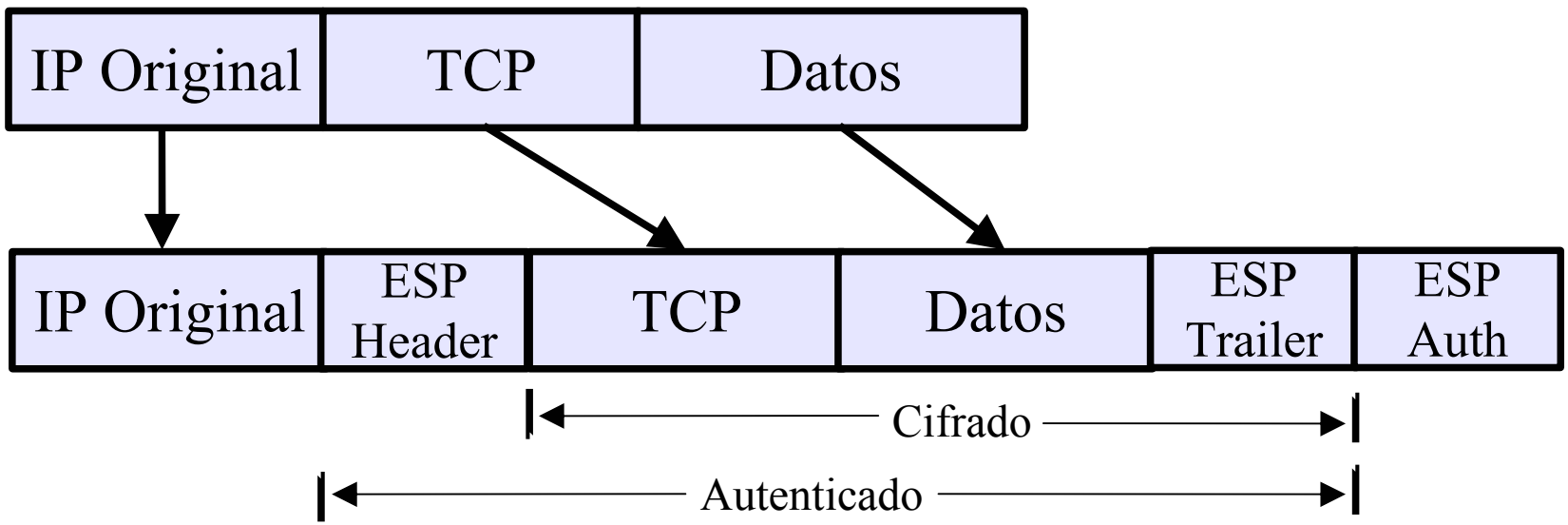
- ***Next Header – Tipo del siguiente encabezado después del AH.***
- ***Payload Length – Longitud de AH en palabras de 32 bits.***
- ***Security Parameters Index – Un valor arbitrario que en combinación con la IP de destino y el protocolo de seguridad, identifica de manera única a la SA.***
- ***Sequence Number – Números de secuencia de paquete. Se inicializa a 0 cuando se establece la SA.***
- ***Authentication Data – Campo de longitud variable que contiene el ICV (Integrity Check Value).***

Integrity Check Value - ICV

- ***Se utilizan como algoritmos:***
  - ***MAC basados en algoritmos de cifrado simétrico (DES-CBC)***
  - ***Funciones de hash: MD5 o SHA-1.***
- ***Se calcula sobre:***
  - ***Campos del encabezado IP que son inmutables durante el tránsito.***
  - ***El encabezado AH (Next Header, Payload Len, Reserved, SPI, Sequence Number)***
  - ***Los datos del protocolo superior.***

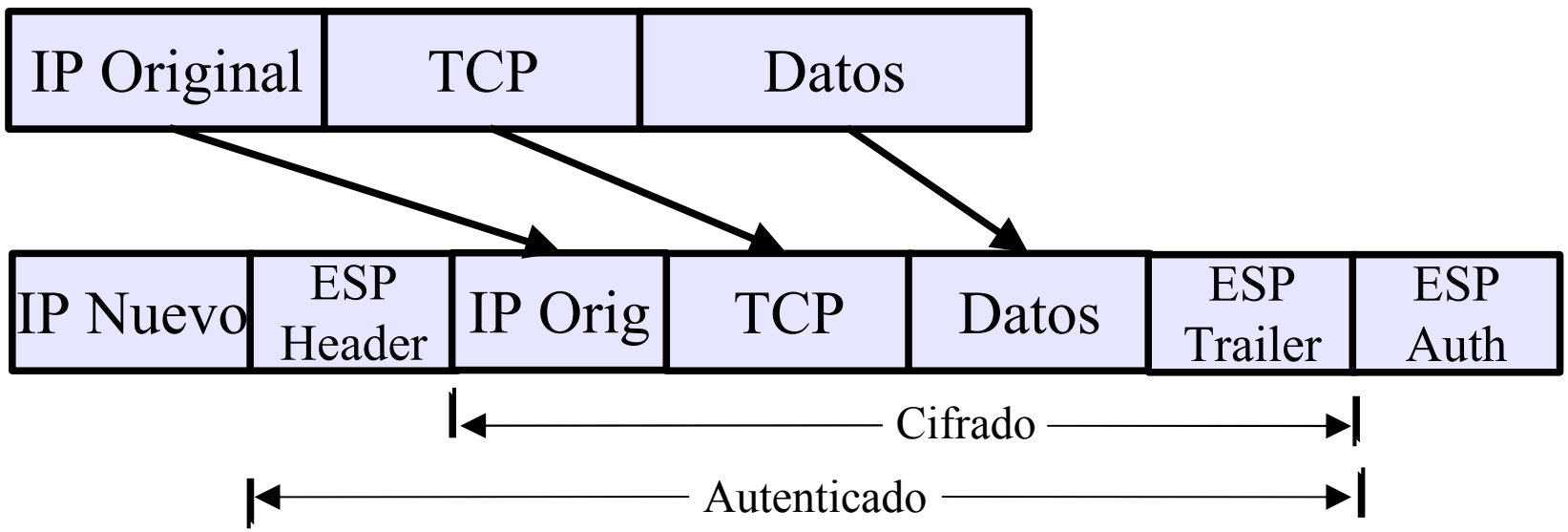
Encapsulating Security Payload

- ***Encapsulating Security Payload (ESP) – Proporciona confidencialidad, integridad y autenticación de origen.***
- ***Modo de transporte:***



Encapsulating Security Payload

- ***Modo de túnel:***



ESP

- ESP Header – Esencialmente los mismos campos del AH Header.
- ESP Auth – Contiene el ICV
- Algoritmos utilizados (obligatorios):
  - DES - CBC
  - HMAC con MD5
  - HMAC con SHA-1
  - Algoritmo de autenticación NULL
  - Algoritmo de cifrado NULL (RFC 2410)
- Algunas implementaciones de IPSec soportan 3DES.

Internet Key Exchange - IKE

- ***Protocolo estándar de manejo de claves utilizado en IPSec.***
- ***IPSec puede trabajar sin IKE (pero no es recomendable).***
- ***IKE es un protocolo híbrido que implementa:***
  - ***Intercambio de claves Oakley y Skeme.***
  - ***ISAKMP (Internet Security Association and Key Management Protocol)***
    - ***Marco de referencia que define formatos de payloads, mecánica de intercambio de claves y la negociación de una asociación de seguridad.***

Internet Key Exchange - IKE

- ***IKE proporciona:***
  - ***Elimina la necesidad de especificar manualmente los parámetros de seguridad de IPSec.***
  - ***Permite especificar un tiempo de vida para una SA.***
  - ***Permite el intercambio de claves durante una sesión IPSec.***
  - ***Proporciona servicio anti-réplica.***
  - ***Soporta AC para implementar IPSec escalable.***
  - ***Permite autenticación dinámica de pares.***

Internet Key Exchange - IKE

- ***IKE implementa:***
  - ***DES y DES-CBC***
  - ***Diffie-Hellman***
  - ***MD5 (variante HMAC)***
  - ***SHA (variante HMAC)***
  - ***Firmas RSA y nonces cifrados con RSA***
  - ***Interoperabilidad con certificados digitales X509v3***
  - ***Algunas implementaciones incorporan cifrado oportunístico***
- ***Se puede realizar autenticación mediante:***
  - ***Firmas digitales***
  - ***Cifrado con clave pública***
  - ***Clave pre-compartida (pre-shared key)***
  - ***Kerberos V (extensión del estándar)***

Fases de IKE

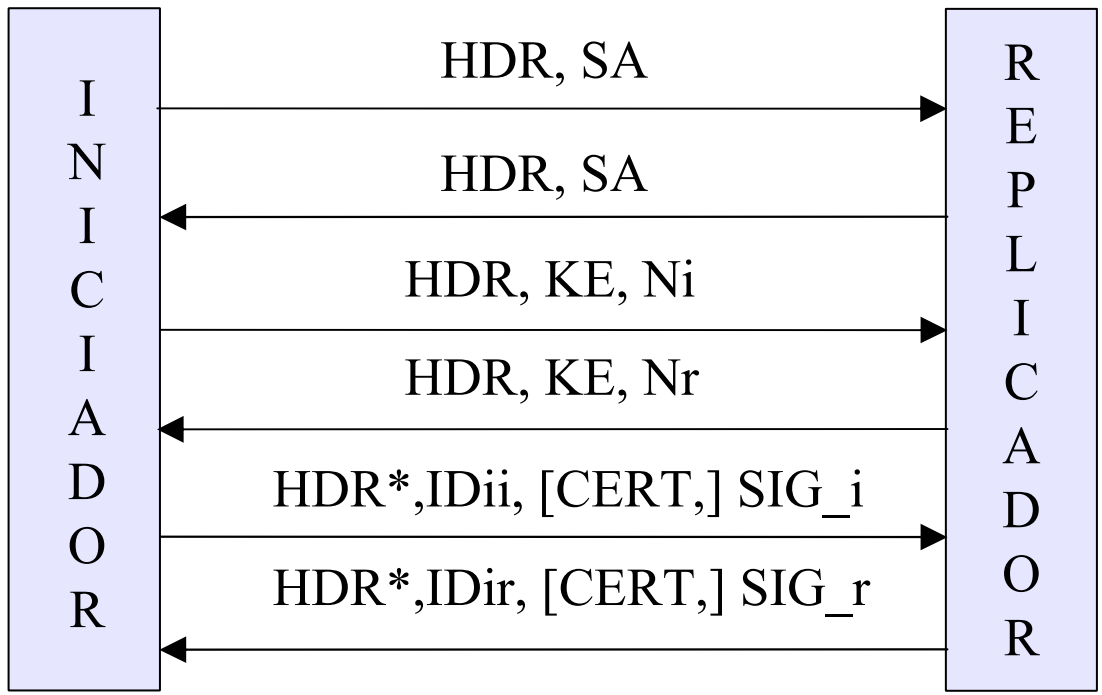
- ***IKE opera en dos fases:***
  - ***Fase I o main mode:***
    - ***1) Negociación de:***
      - ***Algoritmo de cifrado (DES o 3DES)***
      - ***Algoritmo de integridad (MD5 o SHA1)***
      - ***Grupo de Diffie-Hellman***
      - ***Método de autenticación***
    - ***2) Intercambio de clave pública***
    - ***3) Autenticación***

Fases de IKE

- ***IKE opera en dos fases:***
  - ***Fase II o quick mode:***
    - ***1) Negociación de:***
      - ***Protocolo IPSec (AH o ESP)***
      - ***Algoritmo de integridad (MD5 o SHA1)***
      - ***Algoritmo de cifrado (DES o 3DES)***
    - ***2) Establecimiento de clave de sesión.***
    - ***3) Las SA y las claves, junto con el SPI, se pasan a la capa de IPSec.***

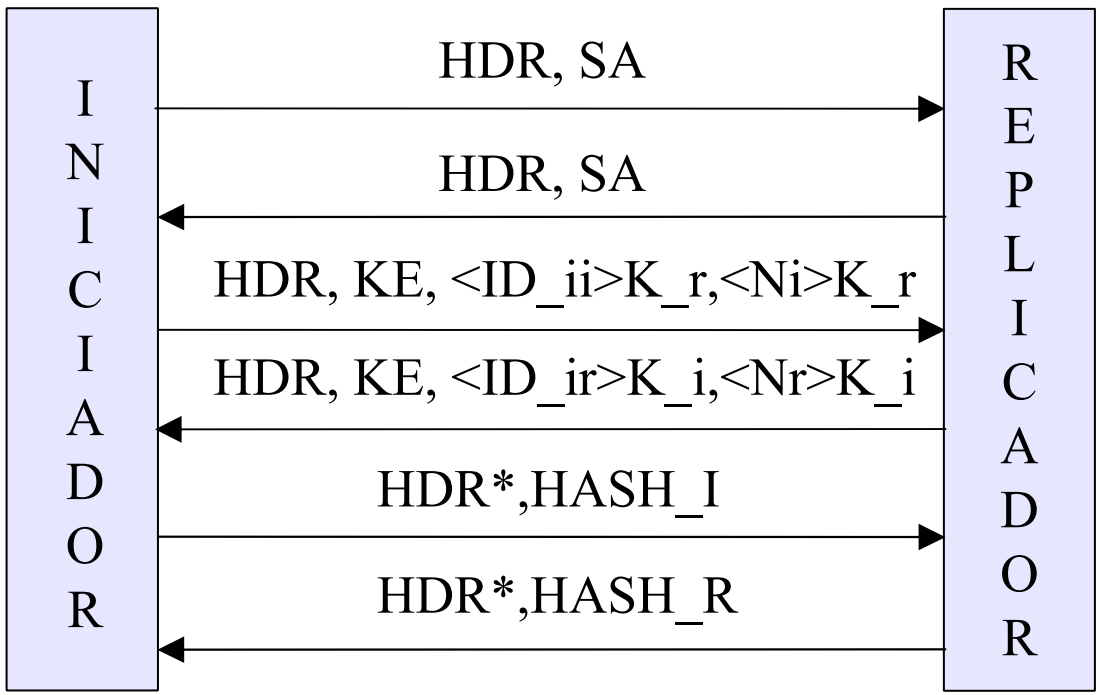
Autenticación por Firmas

- Fase 1 de IKE
  - Modo principal



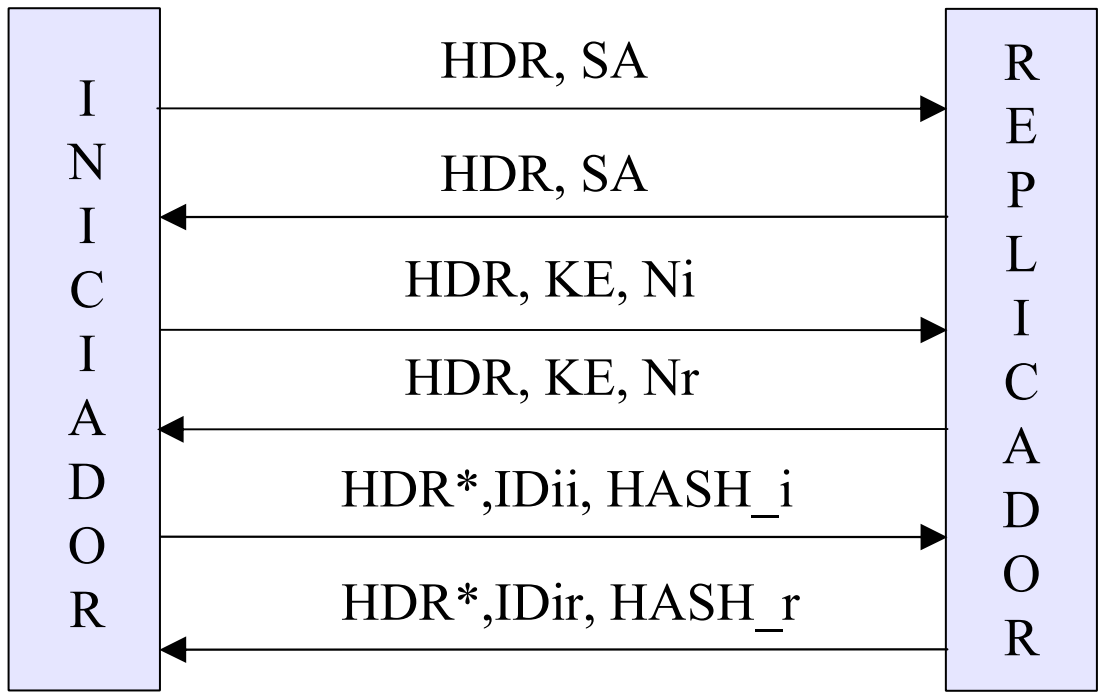
Autenticación por Cifrado

- Fase 1 de IKE
  - Modo principal

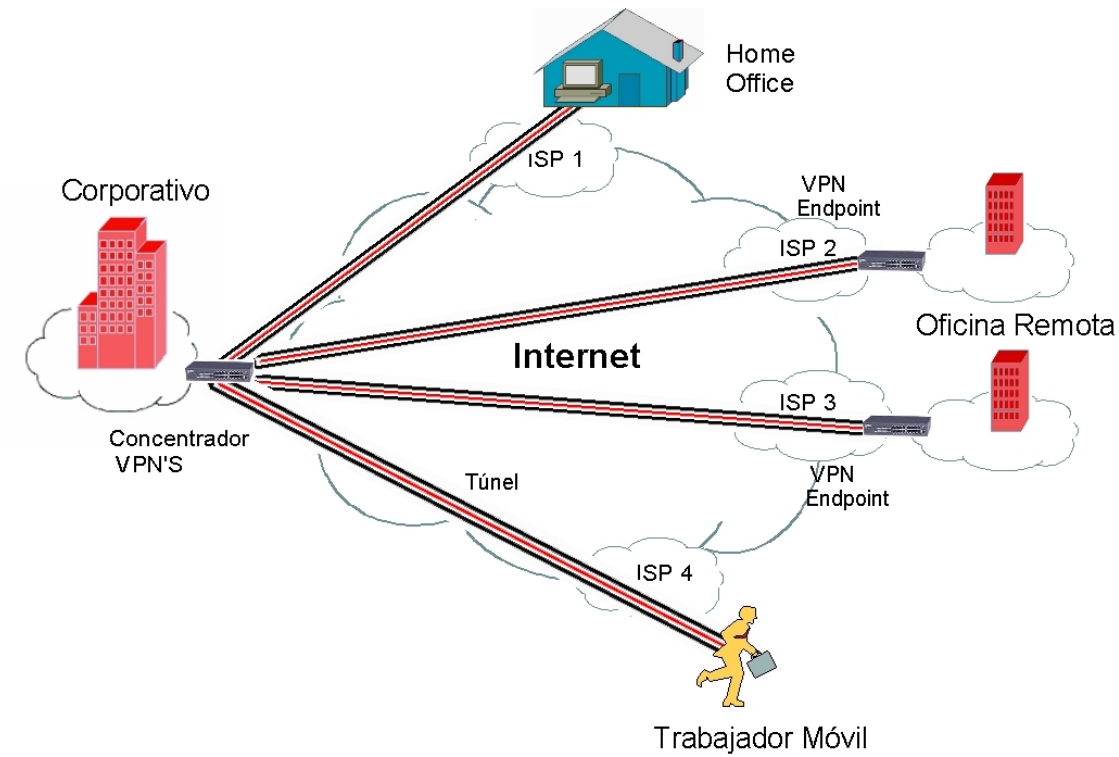


Autenticación por Clave Compartida

- Fase 1 de IKE
  - Modo principal



Redes Privadas Virtuales



Gracias por su atención

http://www.sekureit.com