Seguridad y Competencias Profesionales
Tema 9: Seguridad en redes
Curso 2012–2013

Ingeniería en Informática (2° ciclo)

Departamento de Ingeniería Informática
Universidad de Cádiz

Cádiz, 17 diciembre 2012

Índice

1 Introducción

2 Aplicaciones de autenticidad

3 Seguridad en el correo electrónico

4 Seguridad en la web

5 Proxy y cortafuegos

6 Seguridad en redes inalámbricas

Concepto de seguridad en red

Consiste en establecer medidas para disuadir, prevenir, detectar, y corregir las violaciones de la seguridad que implican la transmisión y el almacenaje de la información a través de la red.

- Garantizar integridad y confidencialidad de las comunicaciones
- Implantar un sistema de autenticación de usuarios
- Control de acceso a servicios ofrecidos y a equipos
- Control del uso de los servicios públicos
- Garantizar la disponibilidad de los servicios

Causas de las vulnerabilidades

- Las comunicaciones por la red sufren los cuatro tipos de amenazas: interrupción, modificación, interceptación y fabricación
- La inseguridad es una parte intrínseca de Internet
- El administrador suele ocuparse del sistema local y no de la red
- Equipos antiguos sin muchos medios para establecer seguridad
- Equipos nuevos preinstalados sin nada configurado para dar seguridad
- Software con *bugs*

Intrusos en la red (I)

Whitehat Se dedican a entrar en sistemas informáticos para demostrar y probar su inteligencia y conocimientos, pero no pretenden provocar daños en el sistema.

Blackhat o *cracker*. Atacan el sistema con el fin de obtener beneficios o provocar daños a la organización (Vladimir Levin, Kevin Mitnick)

Sniffer Rastrea y trata de recomponer y descifrar los mensajes que circulan por redes de ordenadores

Phreaker Especializado en sabotear redes telefónicas para la realización de llamadas gratuitas (John Draper, Kevin Poulson)

Intrusos en la red (II)

Spammer Envían masivamente miles de mensajes de correo electrónico no solicitado, con el fin de colapsar los servidores u obtener beneficios económicos

Lamer *script kiddy* o *click kiddy*. Obtienen programas para realizar ataques informáticos y los utilizan sin tener conocimientos técnicos de cómo funcionan

¿Cómo establecer la seguridad en la red?

Defensa de la organización

Equipo a equipo Cada equipo conectado a la red debe estar perfectamente configurado y asegurado. Estrategia difícil de poner en práctica

Perimetral Crear una barrera entre la red interna de la organización y el exterior. La defensa está centrada en pocos equipos.

Defensa del servidor web

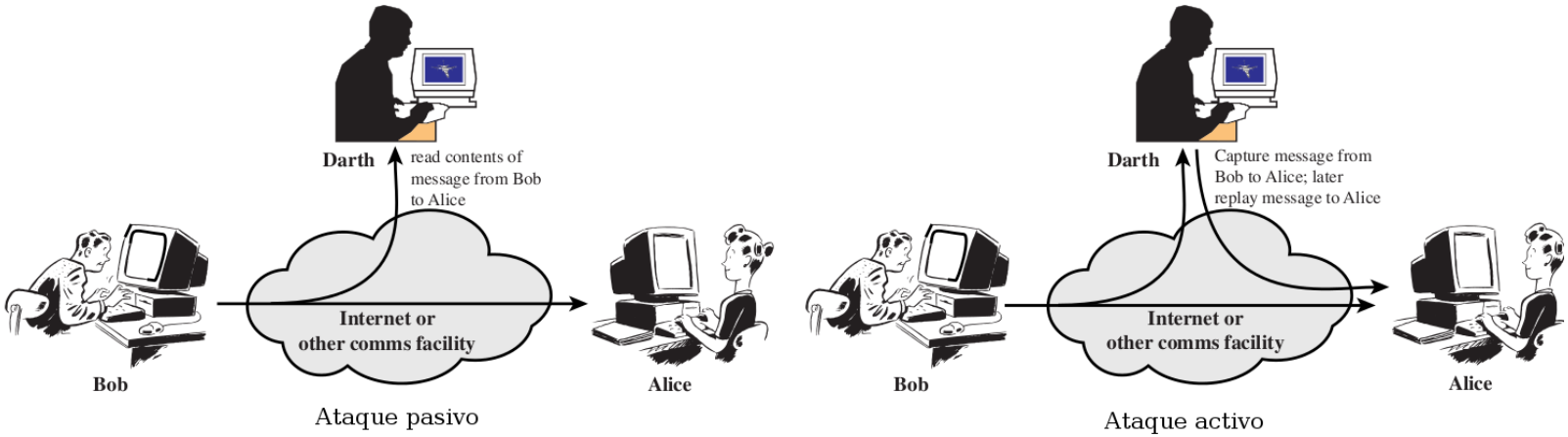
Servidor propio Conectado directamente a Internet

Hosting u hospedaje. El servidor se encuentra en una máquina del proveedor, pudiendo estar compartido con otras empresas

Housing Ubicación de un ordenador propiedad de la empresa en una sala especialmente acondicionada por el proveedor de acceso a Internet

Tipos de ataque

Recomendación X.800 "Security Architecture for OSI" define una manera sistemática para definir y proporcionar los requisitos de seguridad



Ataques pasivos

- Interceptación del tráfico sin modificarlo (*eavesdropping*)
- Reconocimiento del sistema: escaneo de puertos, reconocimiento de versiones de sistema operativo y aplicaciones
- Interceptación de correos y documentos enviados por la red

Características

- Difíciles de detectar: no implican ninguna alteración de los datos.
- El emisor y el receptor no son conscientes del ataque.
- Prevención del éxito de estos ataques mediante encriptación de datos.

Ataques activos (I)

Suplantación de identidad

IP Spoofing Modifica la cabecera de los paquetes enviados a un sistema (RFC 2267)

Hijacking Secuestro de sesiones establecidas: suplanta la dirección IP de la víctima y el número de secuencia del siguiente paquete a transmitir

DNS Spoofing Falsifica el DNS con el fin de realizar un direccionamiento erróneo en los equipos afectados (otras páginas web o interceptar correo)

SMTP Spoofing o *masquerading*. Envío de mensajes con remitentes falsos

Snooping Observar la actividad de un usuario para obtener contraseñas

Ataques activos (II)

Ataques de repetición (*replay attacks*)

Reenvío de mensajes modificados previamente transmitidos

Modificación del tráfico y tablas de encaminamiento

Desviar los paquetes de su ruta original para facilitar la interceptación

Cross-Site Scripting

Ejecución de código script arbitrario en un navegador, con objeto de obtener identificadores de usuarios y modificar contenidos para engañar al usuario

Ataques contra sistemas criptográficos

Ataques activos (III)

Denegación de servicio (DoS)

Consiste en colapsar los equipos y las redes para impedir ofrecer los servicios.

- Ejecutar actividades con alto consumo de recursos (envío de ficheros de gran tamaño)
- Generar grandes cantidades de tráfico desde múltiples equipos
- Transmitir paquetes malformados para caer equipos no preparados
- Falsificar tablas de encaminamiento para impedir el acceso a determinados equipos
- *Mail bombing* Envío masivo de miles de mensajes de correo electrónico

Ataques activos (IV)

Denegación de servicio (DoS) (cont.)

- Ataque reflector (*reflector attack*): generar un intercambio ininterrumpido de tráfico entre dos o más equipos
- Incumplimiento de reglas de protocolo:
  - El ping de la muerte (ping -l 65510 direccion)
  - *Land attack*: Destino y origen iguales.
  - *Supernuke* o *winnuke*: paquetes UDP del tipo *Out-Of-Band* al puerto 137
  - *SYN flood*: No responder a la aceptación de conexión.
  - *Smurf* o pitufo: envío de mensajes de control ICMP de solicitud de eco a direcciones de difusión, etc.

Phishing

Obtención del número de cuenta y claves de acceso a servicios bancarios

Ataques activos (V)

Pharming

Conecta a la víctima páginas falsas simulando las legítimas

Ransom-ware

Software malicioso que al acceder a un sistema codifica los ficheros y exige dinero para restaurarlos

Características

- Difíciles de prevenir: gran cantidad de vulnerabilidades de software y hardware.
- Objetivo: detectar estos ataques cuanto antes para subsanar los daños que han provocado.

Amenazas

- Los usuarios desean tener acceso a servicios en los servidores.

Tipos de amenazas

- El usuario finge ser otro usuario.
- El usuario altera la dirección de red de un sitio de trabajo.
- El usuario escucha la conversación y utiliza una repetición de mensajes antiguos.

Autenticación de usuarios

Problemas

- Autenticidad del emisor
- Integridad del emisor
- Actualidad del mensaje
- No repudio del emisor
- No repudio del receptor
- Usurpación de identidades

Esquema de soluciones

Basados en criptografía simétrica

- Kerberos
- Autenticación de mensajes MACs

Basados en criptografía asimétrica

- Servicio de directorios X.509

Kerberos (I)

Descripción

- Servicio de autenticación desarrollado en 1988 en el MIT.
- "Kerberos" es un personaje mitológico griego: el perro guardián de tres cabezas.
- Proporciona un intercambio de claves con una tercera parte de confianza:
  - Todos confían en el servidor central de autenticación.
  - Basado en el protocolo de distribución de claves de Needham & Schroeder.
- Dos versiones funcionando:
  - Versión 4: utiliza DES, en un protocolo bastante elaborado, para proporcionar el servicio de autenticación. Es la versión "original".
  - Versión 5: utiliza AES.

Kerberos (II)

Requisitos

Seguro Un observador de la red no debería poder obtener la información necesaria para hacerse pasar por un usuario.

Fiabilidad Debería ser muy fiable y emplear una arquitectura de servidores distribuida en la que un sistema pudiera disponer de copias de otro.

Transparencia Aparte del requisito de introducir una contraseña, el usuario no debería ser consciente de la autenticación.

Escalabilidad Debería dar cabida a un gran número de clientes y servidores (arquitectura distribuida).

Kerberos (III)

Características

- Kerberos se centra en que cada usuario debe identificarse cada vez que solicita un servicio.
- Autenticación mutua: tanto cliente como servidor verifican la identidad uno del otro.
- Credenciales basadas en:

  Ticket Sirve para pasar la identidad entre el cliente y el servidor

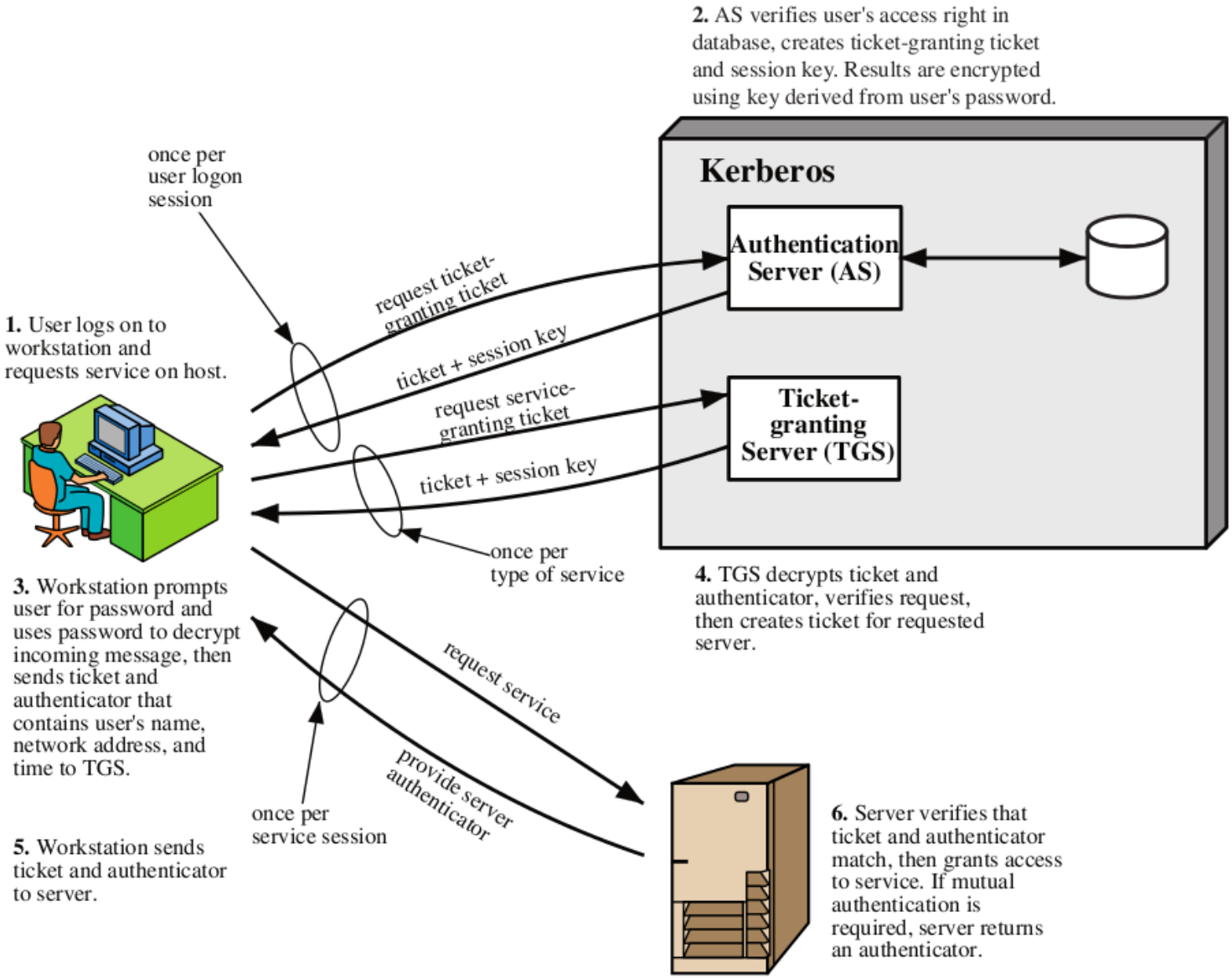
  Autenticador Comprueba que el cliente es el dueño del ticket.

Elementos

- Cliente y servidor
- Servidor de Autenticación (AS)
- Servidor de Ticket Garantizados (TGS)

Kerberos (IV)

Esquema de funcionamiento



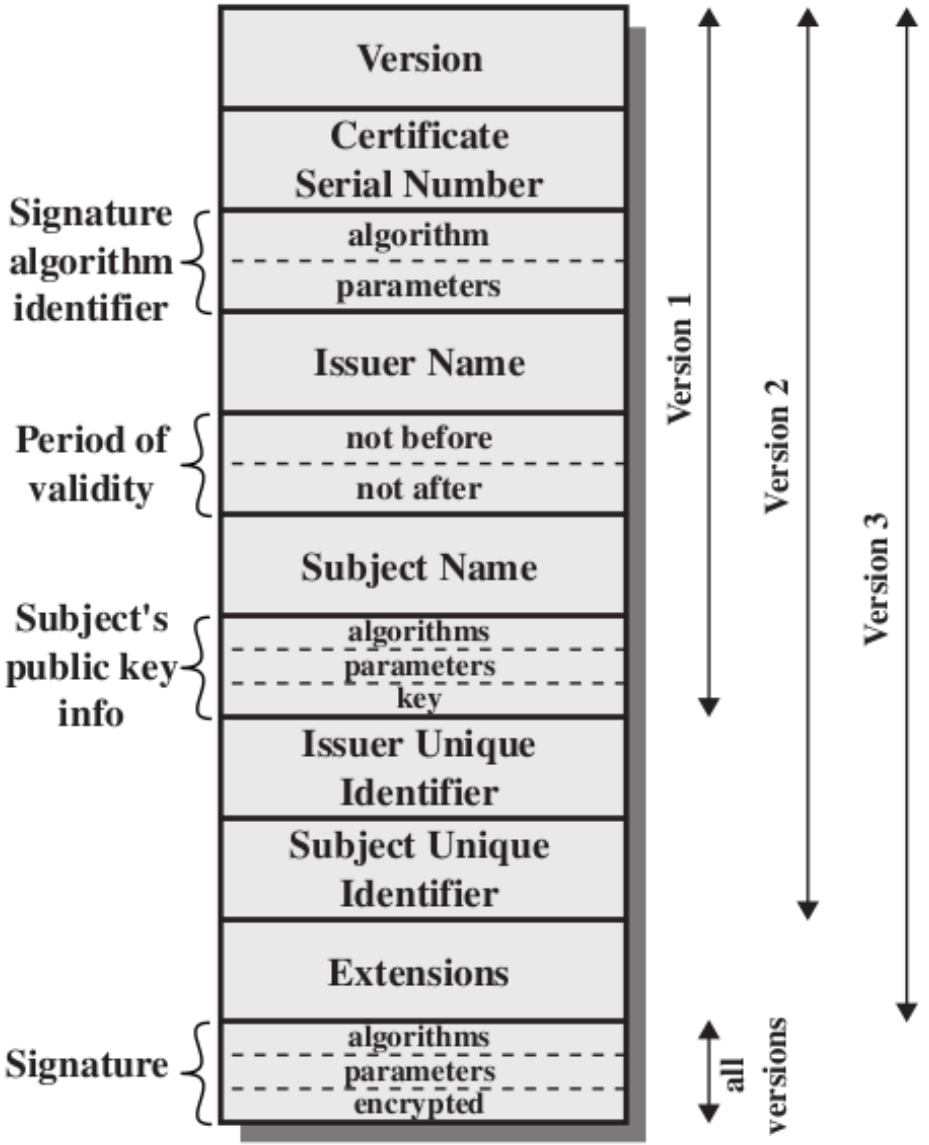
Servicio de directorios X.509 (I)

Características

- Basado en criptografía asimétrica y la existencia de una autoridad certificadora (CA).
- CA es una entidad que emite certificados digitales para uso de terceros.
- Sistema distribuido de servidores que mantiene una base de datos sobre usuarios (certificados).
- Aparece en 1988, revisiones en 1993, 1995, 2000 y 2008.
- Cada certificado contiene la llave pública de un usuario y se firma con la llave privada de un CA.
- Se utiliza en seguridad de S/MIME, del IP, SSL/TLS y SET.
- Se recomienda utilizar algoritmo RSA.

Servicio de directorios X.509 (II)

Formato del certificado X.509

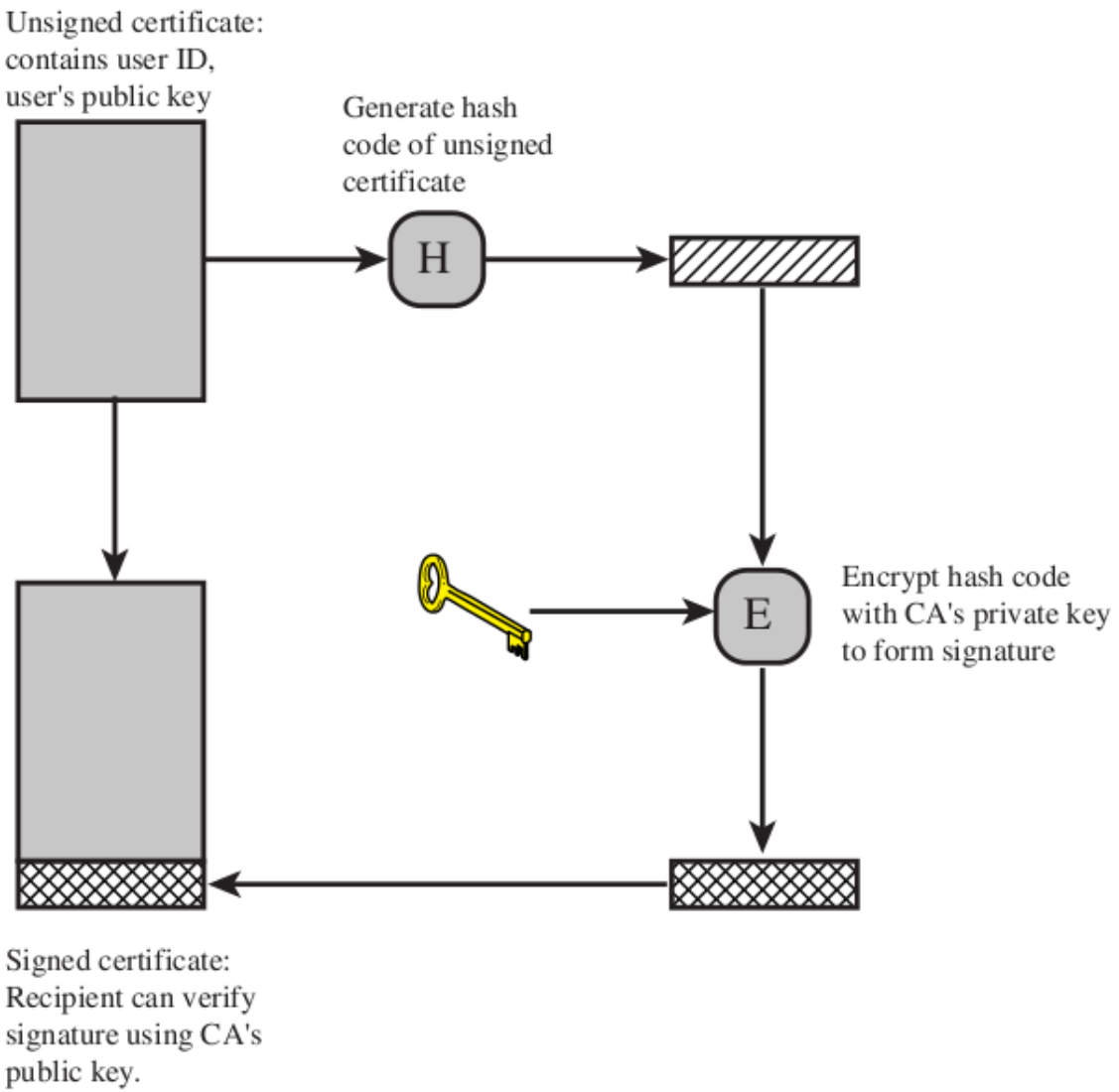


Certificados (I)

Generación del certificado

- Cualquier usuario con el acceso a la llave pública del CA puede verificar la llave pública del usuario que fue certificada.
- Nadie, a excepción del CA, puede modificar el certificado sin que éste sea detectado.

Certificados (II)
Generación del certificado



Certificados (III)
Tipos

Certificados de usuario final

Clase 1 CA	Integrados en una tarjeta. Nivel más alto de seguridad
Clase 1S CA	Requiere de un software para hacer las operaciones sobre el certificado que se encuentra en la tarjeta
Clase 2 CA	No requiere de software adicional, se realiza con el navegador
Clase 3 CA	Igual que el CA pero sin autenticación de usuarios

Certificados (III)
Tipos

SCP T9

Ingeniería en Informática (2° ciclo)

Introducción

Aplicaciones de autenticidad

Seguridad en el correo electrónico

Seguridad en la web

Proxy y cortafuegos

Seguridad en redes inalámbricas

Certificados de firma de software

- Verifican los productos software desarrollados por una empresa.
- Se utilizan integrados con herramientas de firma de software como MS Authenticode, Netscape Signing Tools, etc.

Certificados de servidores SSL

- Autenticidad de un servidor.
- Se integra en servidores que soporten protocolo SSL.

Certificados (IV)

Utilidades

- Sellado temporal de mensajes (ISOIEC 18014): al mensaje a transmitir añade un campo con fecha en formato UTC que es firmada por la clave privada del notario digital.
- Notificaciones telemáticas
- Custodia segura de documentos electrónicos
- Firma de contratos electrónicos
- Sistemas de voto electrónico seguro

PGP versus GPG

Utilidades

- PGP y GPG son las herramientas para establecer confidencialidad y autenticidad tanto a nivel de correo electrónico como de almacenamiento de ficheros.
- PGP es software privativo.
- GPG es software libre (proyecto GNU).

GPG (I)

Características

- Disponible para muchas plataformas.
- Ambos emplean algoritmos bien conocidos: PGP son algoritmos patentados, mientras que GPG tiene todo bajo licencia GNU GPL.
- Amplia gama de usos e interfaces (Seahorse para GNOME, FireGPG para Firefox).
- No está controlado por organizaciones gubernamentales o de estándares.
- Cumple el estándar RFC 2440 de gestión de claves.

GPG (II)

Los servicios proporcionados por GPG son:

Autenticación

- Se envía el mensaje junto con un resumen del mismo que está cifrado con la clave privada del emisor
- Firma: MD5, SHA-1, SHA-256, SHA-384, SHA-512, RIPEMD /160
- Cifrado: RSA, El Gamal

Confidencialidad

- Se cifra el mensaje con una clave
- Cifrado mensaje: AES, Triple DES, Blowfish, CAST5, Twofish
- Cifrado clave: RSA con clave pública del receptor

GPG (III)

Los servicios proporcionados por GPG son (cont.):

Compresión

ZIP, ZLIB, ZLIB2

Compatibilidad correo electrónico

Utiliza esquema Radix-64, que expande el mensaje de bloques de 24 a 32 bits.

Segmentación

Automáticamente divide los mensajes que sobrepasan el tamaño máximo en pequeños bloques y luego los vuelve a ensamblar.

S/MIME (I)

Características

- *Secure/Multipurpose Internet Mail Extension*
- S/MIME es el estándar de uso industrial, comercial y empresarial.
- PGP/GPG para seguridad del correo personal.
- S/MIME definido en RFC 2630, 2632 y 2633
- Basado en RSA.

S/MIME (II)

Evolución histórica

- SMTP (RFC 822) tenía limitaciones:
  - Transmisión de ficheros ejecutables
  - Juego de caracteres nacionales
  - Mensajes con líneas de más de 76 caracteres
- MIME (RFC 2045, RFC 2046) supera dichos problemas, pero:
  - No tiene confidencialidad
  - No tiene autenticación

S/MIME (III)

Funciones

- **Datos empaquetados**: mensaje cifrado y uso de claves de sesión por comunicación.
- **Datos firmados**: un resumen del mensaje se cifra con la clave privada del emisor y unido al mensaje se cifra con la pública del receptor.
- **Datos firmados en claro**: firmado pero no cifrado.
- **Datos firmados y empaquetados**: se pueden anidar varios cifrados y firmas en un mismo mensaje.

S/MIME (IV)

Algoritmos empleados

- **Resumen**: SHA-1 y MD5
- **Firmas de Digital**: DSS
- **Cifrado simétrico con clave de sesión**: Triple-DES, RC2/40 (exportable)
- **Cifrado asimétrico Público-Privado**: RSA con claves de 512 y 1024, y Diffie-Hellman (para las claves de sesión).

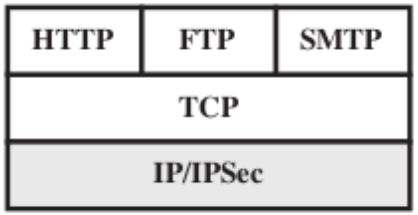
Seguridad en la web

Consideraciones

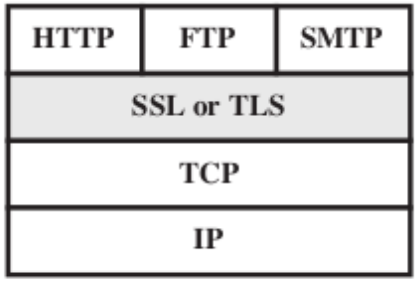
- La Web es muy visible.
- Mucho software complejo y con muchos defectos de seguridad.
- Recibe ataques activos y pasivos.
- Servidores web fáciles de configurar y gestionar.
- Los usuarios no conocen todos los riesgos.

Métodos de asegurar la web

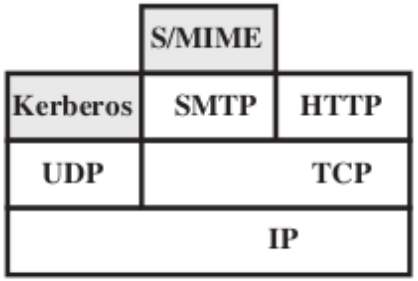
- Seguridad en nivel de red
- Seguridad en nivel de transporte
- Seguridad en nivel de aplicación



(a) Network Level



(b) Transport Level

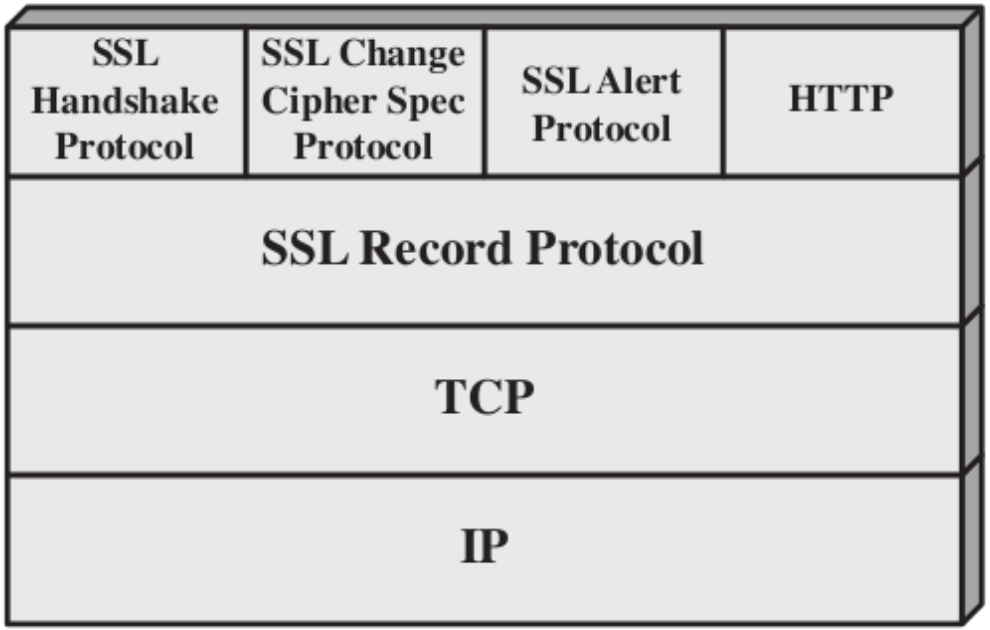


(c) Application Level

SSL/TLS (I)

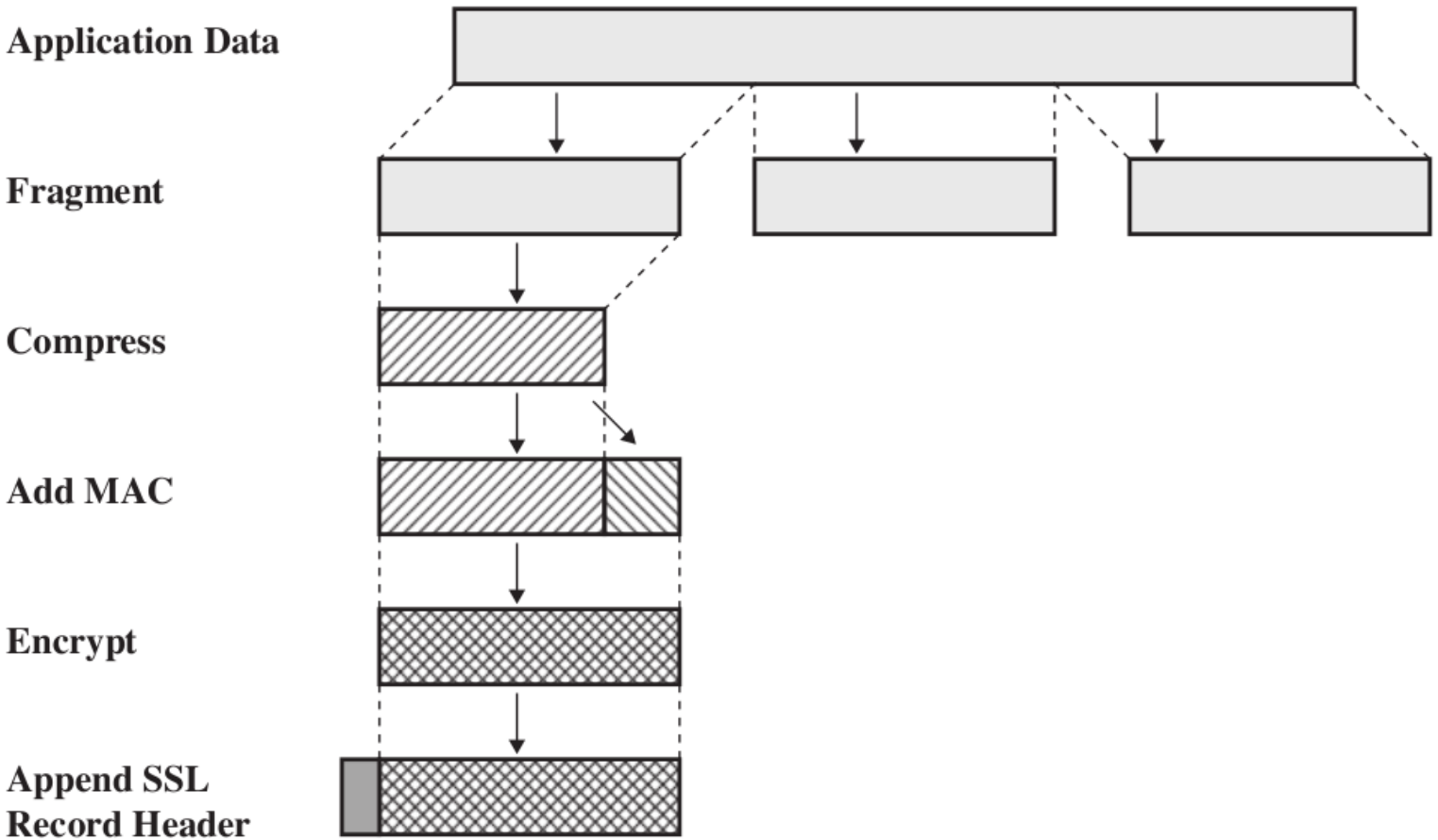
- SSL fue creado por Netscape
- Formaron al grupo de funcionamiento de TLS dentro del IETF
- La primera versión de TLS se puede ver como SSLv3.1

SSL/TLS (II)
Arquitectura

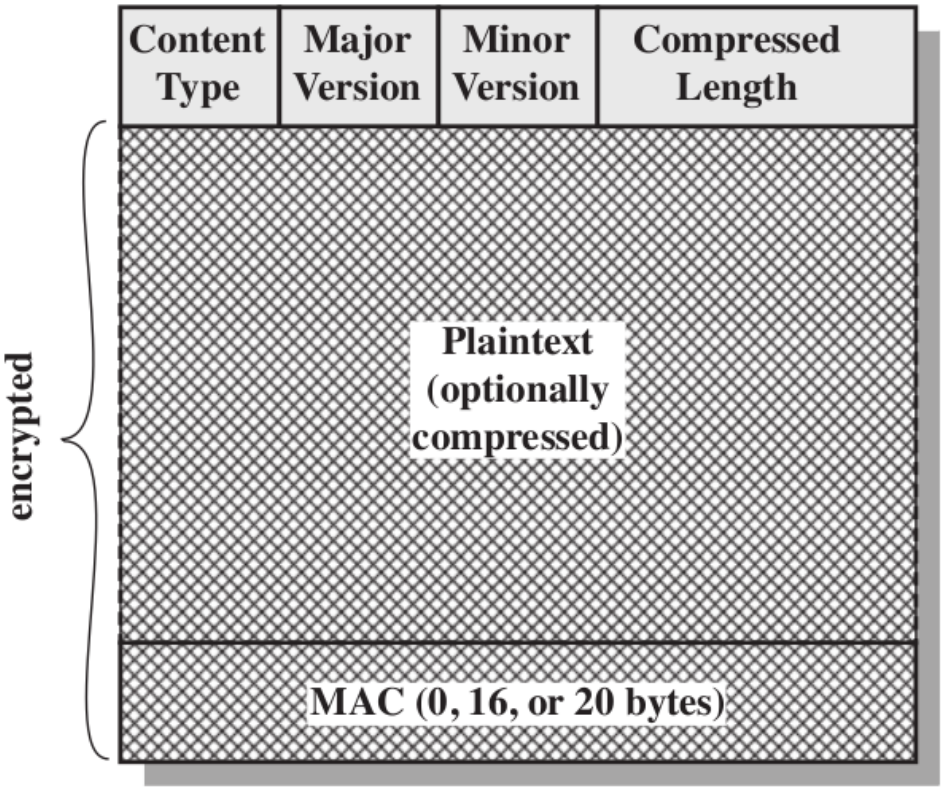


Protocolo Record SSL

Proporciona confidencialidad e integridad.



Formato de mensaje Record SSL

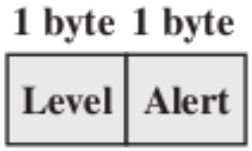


Protocolo Change Cipher Spec

- Es un mensaje de 1 byte con valor 1.
- Objetivo: un estado pendiente pasa a finalizado.

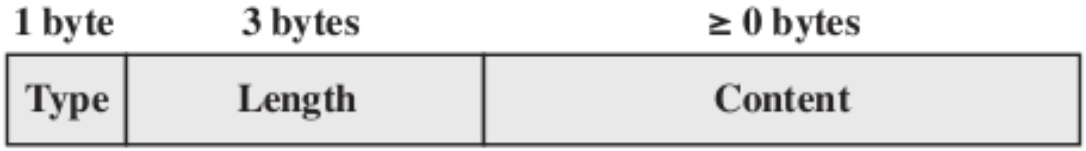
Protocolo Alert

- Objetivo: transmitir las alertas.
- Alertas graves: MAC incorrecto, mensaje inesperado, fallo protocolo, parámetro ilegal.

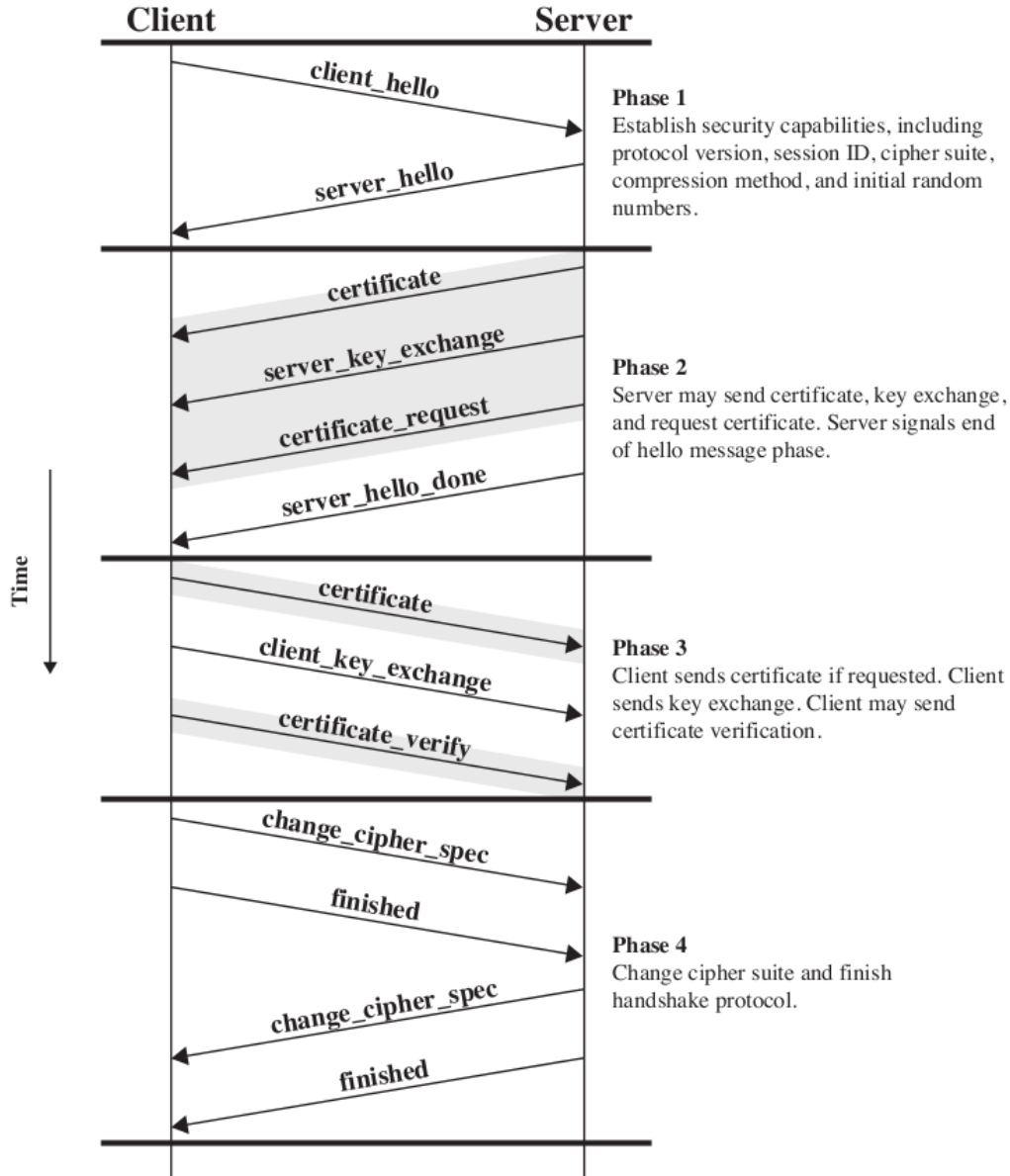


Protocolo Handshake

- Realiza la autenticación entre cliente y servidor.
- Negocia las claves a emplear.
- Es el primero en usarse.



Funcionamiento de protocolo Handshake



SET (I)

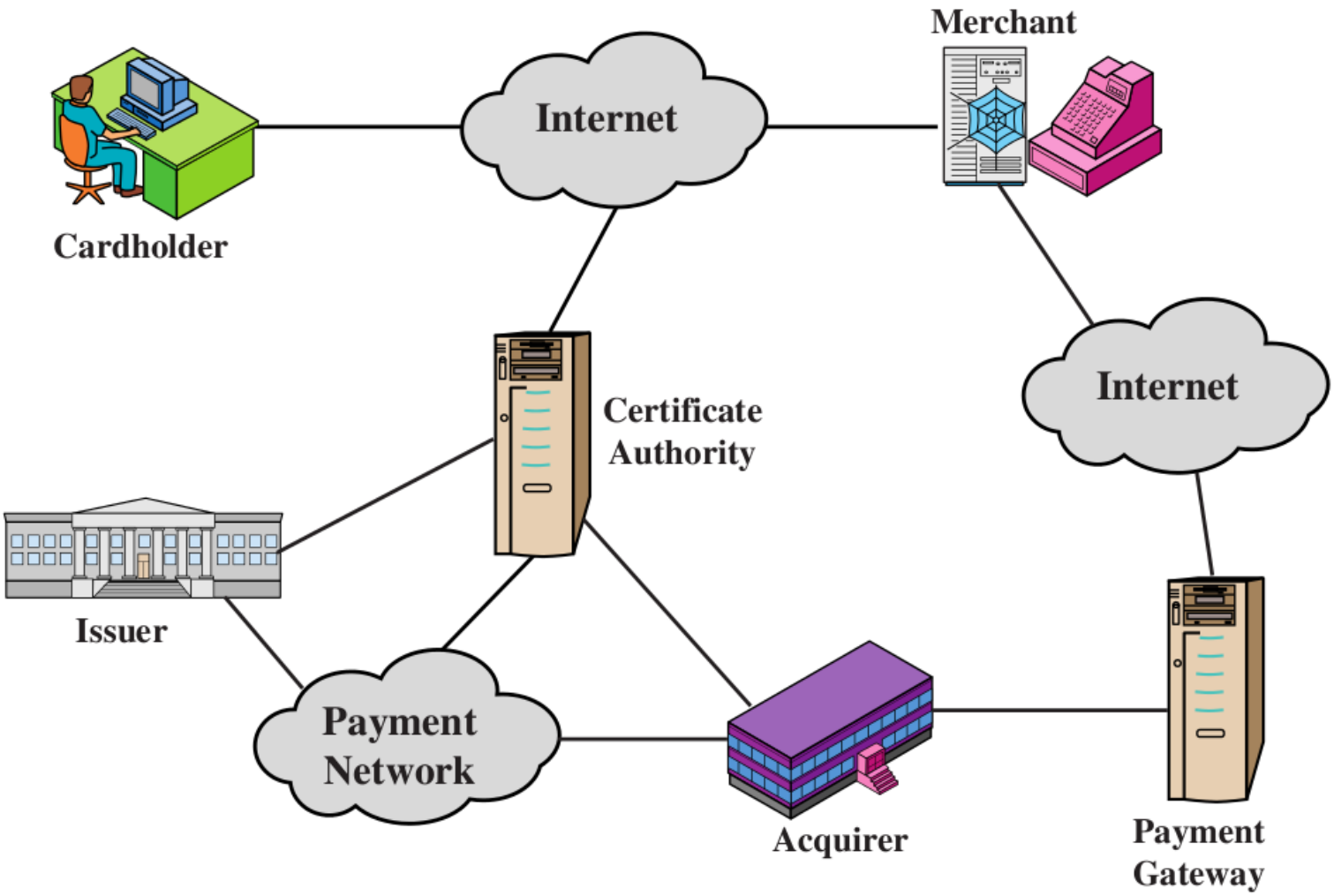
- Transacciones electrónicas seguras.
- Una especificación abierta del cifrado y de la seguridad.
- Proteger las transacciones de las tarjetas de crédito en Internet.
- Compañías implicadas: Mastercard, VISA, IBM, Microsoft, Netscape, RSA, Terisa y Verisign
- No es un sistema de pago.
- Sistema de protocolos y de formatos de la seguridad.

SET (II)

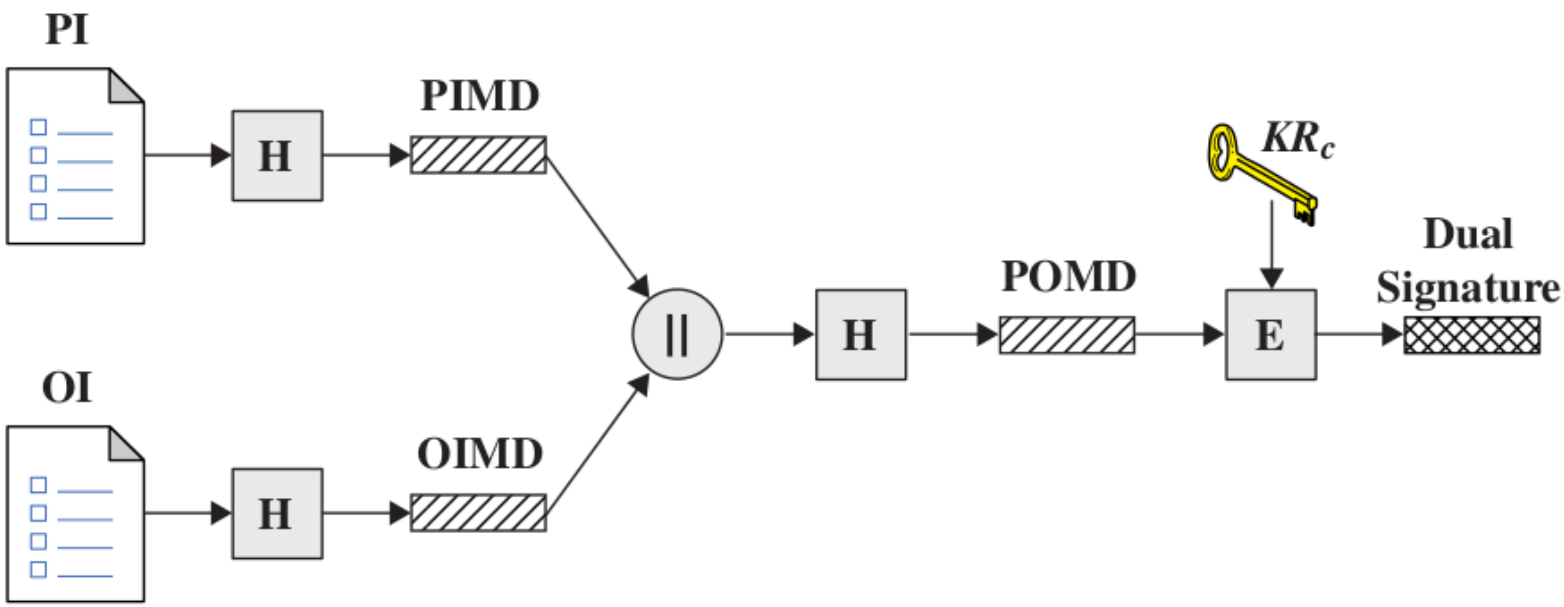
Características

- Confidencialidad del pago y el pedido: DES
- Integridad de las transmisiones: RSA, SHA-1
- Autenticación
- Certificados digitales

SET (III)
Participantes



SET (IV)
Firma dual

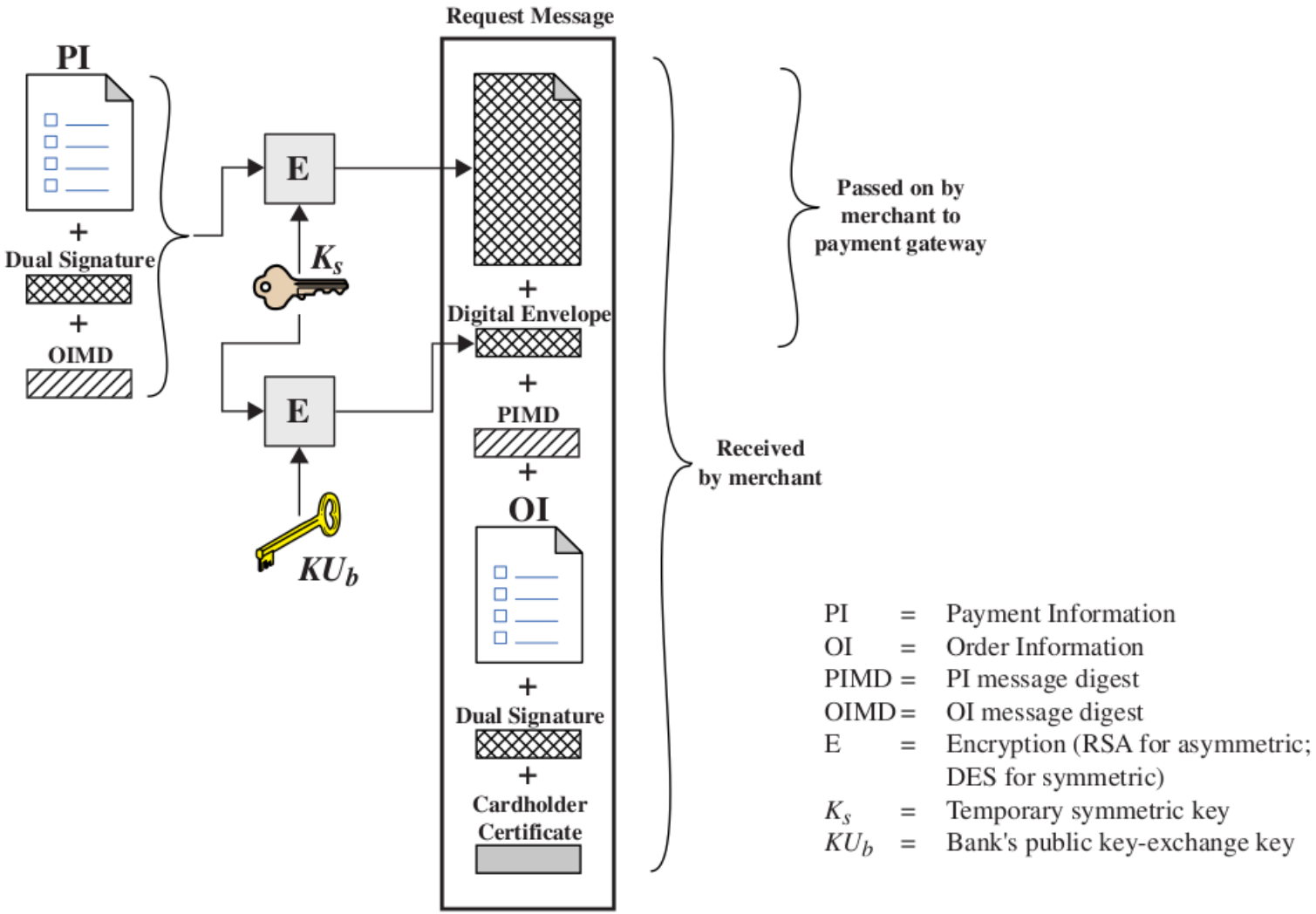


PI = Payment Information
OI = Order Information
H = Hash function (SHA-1)
|| = Concatenation

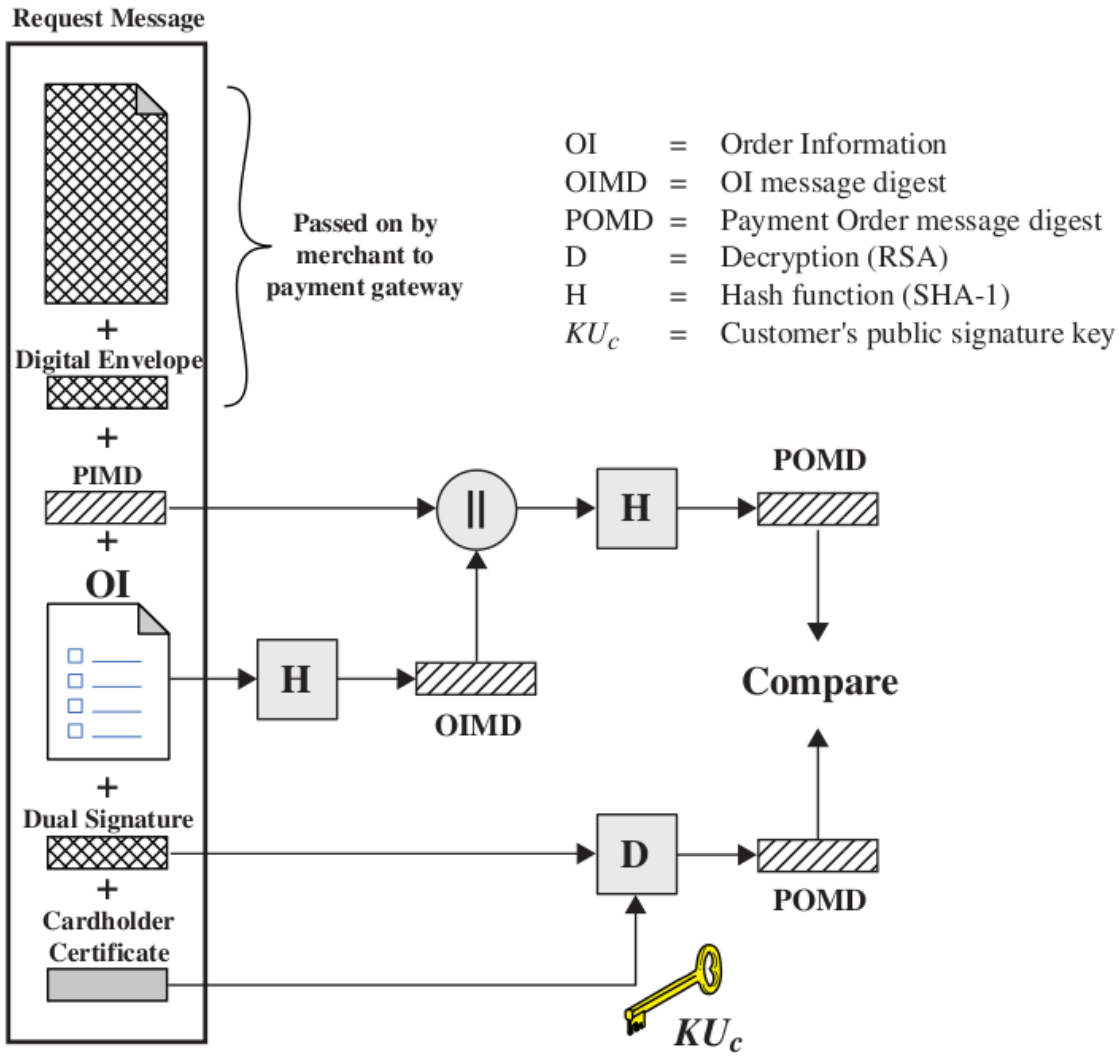
PIMD = PI message digest
OIMD = OI message digest
POMD = Payment Order message digest
E = Encryption (RSA)
KR_c = Customer's private signature key

SET (V)

Solicitud de compra



SET (VI)
Comprobación del cliente



SET (VII)

Procesamiento de pago

- **Autorización del pago**: el vendedor se asegura que la tarjeta es verdadera.
  - Solicitud de autorización
  - Respuesta de autorización
- **Captura de pago**: el vendedor cobra por la operación.
  - Solicitud de captura
  - Respuesta de captura

Servidor Proxy

- Actúa de intermediario entre equipos internos y redes externas, encargándose de realizar las peticiones a los servidores de Internet en nombre de los equipos internos.
- Los servicios externos no conocen el verdadero nombre del equipo que lo solicita, sólo del proxy
  - Definición de permisos de acceso a servicios de Internet
  - Bloqueo de acceso a direcciones IP y dominios de Internet
  - Auditoría de los servicios de Internet usados
  - Filtrado de paquetes (puede estar en el cortafuegos)
  - Instalación de un antivirus perimetral

Cortafuegos o *firewall* (I)

Definición

- Medio eficaz de protección de un sistema o una red local de sistemas contra amenazas a la seguridad a través de la red
- Un punto de control y de supervisión que interconecta redes de confianza
- Impone restricciones al tráfico
- Sólo se permiten los servicios autorizados de la red
- Establece dos zonas de trabajo independientes:
  - Zona fiable con equipos de la red interna
  - Zona no fiable donde están los equipos externos

Cortafuegos o *firewall* (II)

Características generales

- Canaliza todo el tráfico entre la red local e Internet (se bloquea físicamente todo el acceso a la red excepto vía el cortafuego)
- Sólo puede pasar el tráfico autorizado (definido por las Políticas de Seguridad)
- Es inmune a la penetración, empleando un sistema de confianza con un sistema operativo seguro

Cortafuegos o *firewall* (III)

Técnicas generales

- **Control de servicio**: determina los tipos de servicios de Internet a los que se pueden acceder
- **Control de la dirección**: determina qué direcciones pueden emitir solicitudes y cuáles son las direcciones destino
- **Control de usuario**: controla el acceso al servicio en base al usuario (local)
- **Control del comportamiento**: controla el modo de uso de los servicios (filtros de correo electrónico, etc.)

Cortafuegos o *firewall* (V)
Filtrado de paquetes (I)

SCP T9

Ingeniería en Informática (2° ciclo)

Introducción

Aplicaciones de autenticidad

Seguridad en el correo electrónico

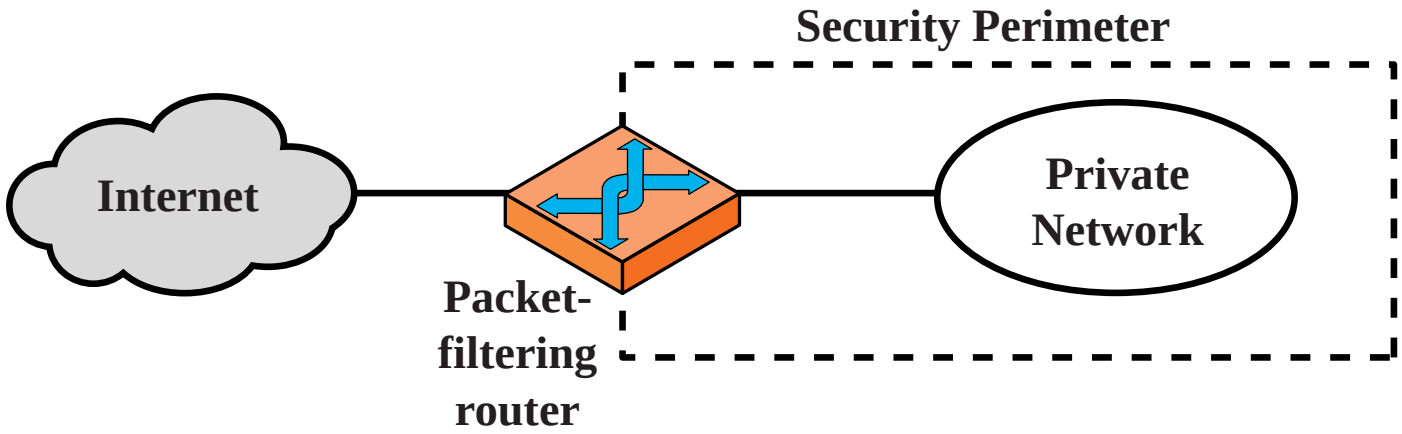
Seguridad en la web

Proxy y cortafuegos

Seguridad en redes inalámbricas

Características

- Aplica un sistema de reglas a cada paquete IP entrante y, entonces, remite o desecha el paquete
- Filtra en ambas direcciones
- Se filtra sobre la información contenida en el paquete: dirección IP origen y destino, puerto, etc.



Cortafuegos o *firewall* (VI)

Filtrado de paquetes (II)

Ventajas

- Simple
- Transparente al usuario
- Rápido

Inconvenientes

- Difícil establecer reglas de filtrado seguras
- Carece de autenticación de usuario (se confía en el equipo)
- Información limitada

Cortafuegos o *firewall* (VII)

Filtrado de paquetes (III)

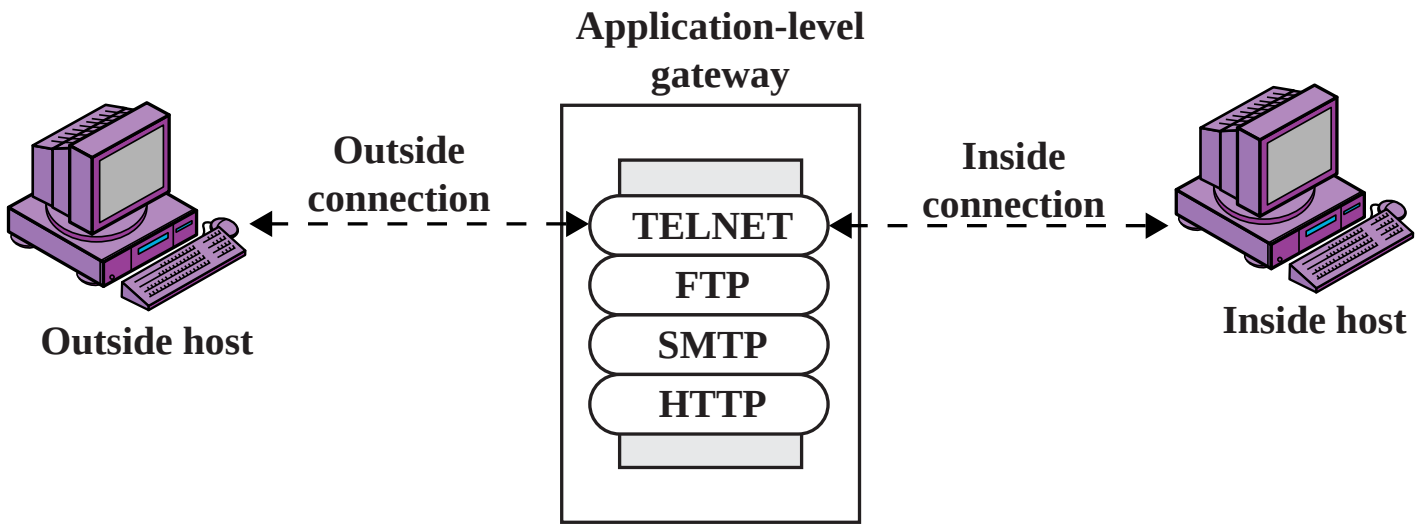
Posibles ataques y contramedidas:

- **Suplantación de dirección IP**: descartar paquetes que provengan de la interfaz externa
- **Ataques de enrutamiento en origen**: descartar paquetes que tengan fijado un enrutamiento que descarte sistemas de seguridad
- **Ataques de fragmento pequeño**: descartar todos los paquetes que tengan desplazamiento de fragmento IP

Cortafuegos o *firewall* (VIII)

Pasarela de nivel de aplicación (I)

- Servidor Proxy
- Actúa como un repetidor del tráfico de nivel de aplicación



Cortafuegos o *firewall* (IX)

Pasarela de nivel de aplicación (II)

SCP T9

Ingeniería en Informática (2° ciclo)

Introducción

Aplicaciones de autenticidad

Seguridad en el correo electrónico

Seguridad en la web

Proxy y cortafuegos

Seguridad en redes inalámbricas

Ventajas

- Mayor seguridad que el filtrado de paquetes
- Sólo escruta unas pocas aplicaciones permitidas
- El tráfico entrante es fácil de registrar y auditar

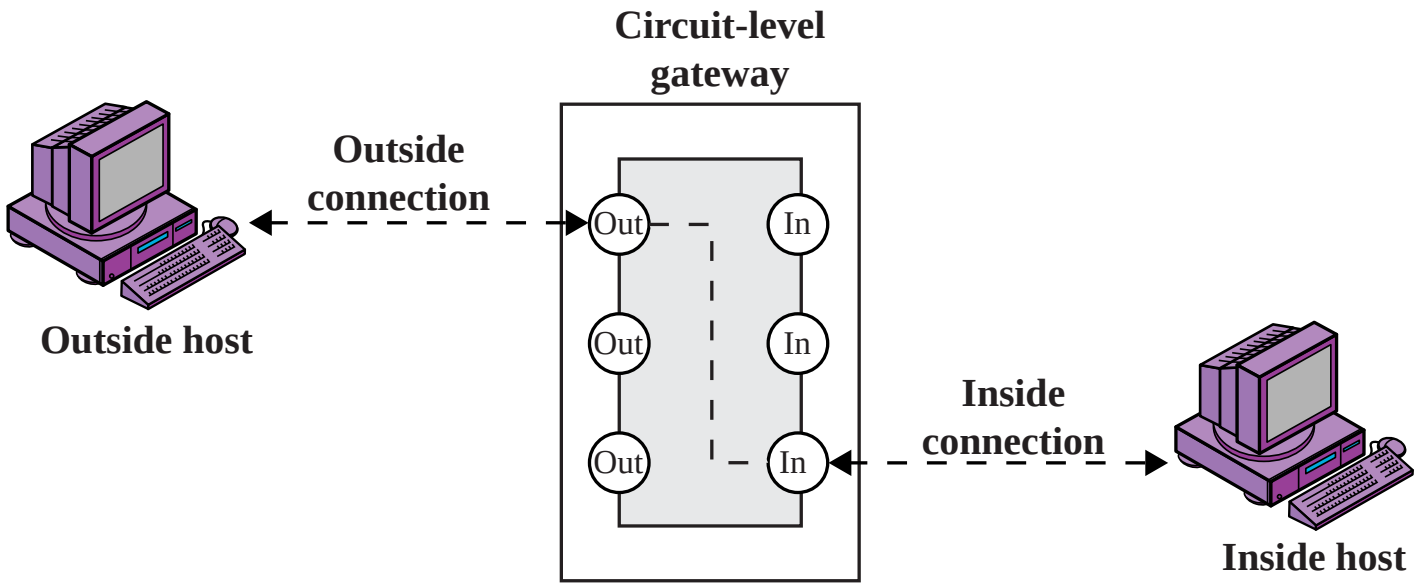
Inconvenientes

- Procesamiento adicional en cada conexión

Cortafuegos o *firewall* (X)

Pasarela de nivel de circuito

- Sistema autónomo o una función especializada de un servidor proxy
- Establece dos conexiones: una con el exterior y otra con el interior
- Repite los segmentos TCP sin examinarlos



Cortafuegos o *firewall* (XI)

Bastión

- Se coloca un ordenador con dos tarjetas de red que separa la red interna de la externa
- Su configuración puede realizar además de filtrados, otras comprobaciones de seguridad

Seguridad en redes inalámbricas (I)

Características

- Transparencia y simplicidad de uso
- Ahorro económico
- Ubicuidad de servicios
- Crecimiento vertiginoso

Seguridad en redes inalámbricas (II)

Problemas

- *Piggybacking*
- *Warchalking*
- *Wardriving*

Piggybacking

Características

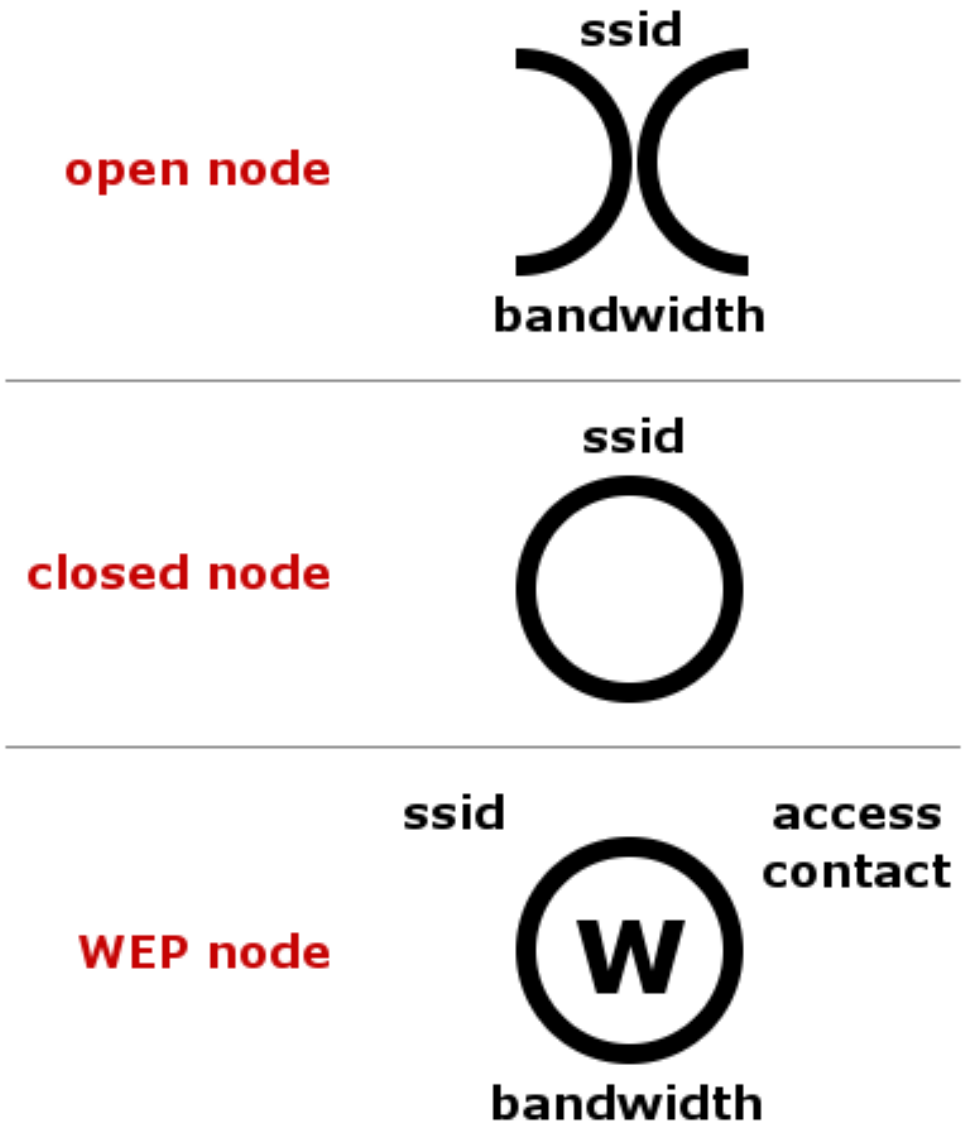
- Uso de una red inalámbrica cercana no protegida
- Problemas:
  - Violaciones del servicio contratado
  - Pérdida de ancho de banda
  - Abuso de usuarios maliciosos
  - Monitorizar la actividad para fines delictivos
  - Atacar nuestros ficheros, instalar virus, etc.

Warchalking (I)

Características

- Consiste en caminar por la calle con un portátil dotado de una tarjeta WLAN, buscando la señal de puntos de acceso.
- Cuando se encuentra uno, se pinta con tiza un símbolo especial en la acera o en un muro, indicando la presencia del punto de acceso y si tiene configurado algún tipo de seguridad o no.
- De este modo, otras personas pueden conocer la localización de la red

Warchalking (II)



Wardriving (I)

Características

- Consiste en localizar puntos de acceso inalámbrico desde un automóvil.
- Se necesita de un computador portátil con una tarjeta WLAN, una antena adecuada, un GPS para localizar los puntos de acceso en un mapa, y software para detección de redes inalámbricas.

Wardriving (II)

Herramientas para redes inalámbricas

- Airsnort
- AirTraf
- FakeAP
- HostAP
- Kismet
- MacStumbler
- Network Stumbler
- WaveStumbler
- Wellenreiter
- WepCrack
- WifiScanner
- ...

Métodos de seguridad

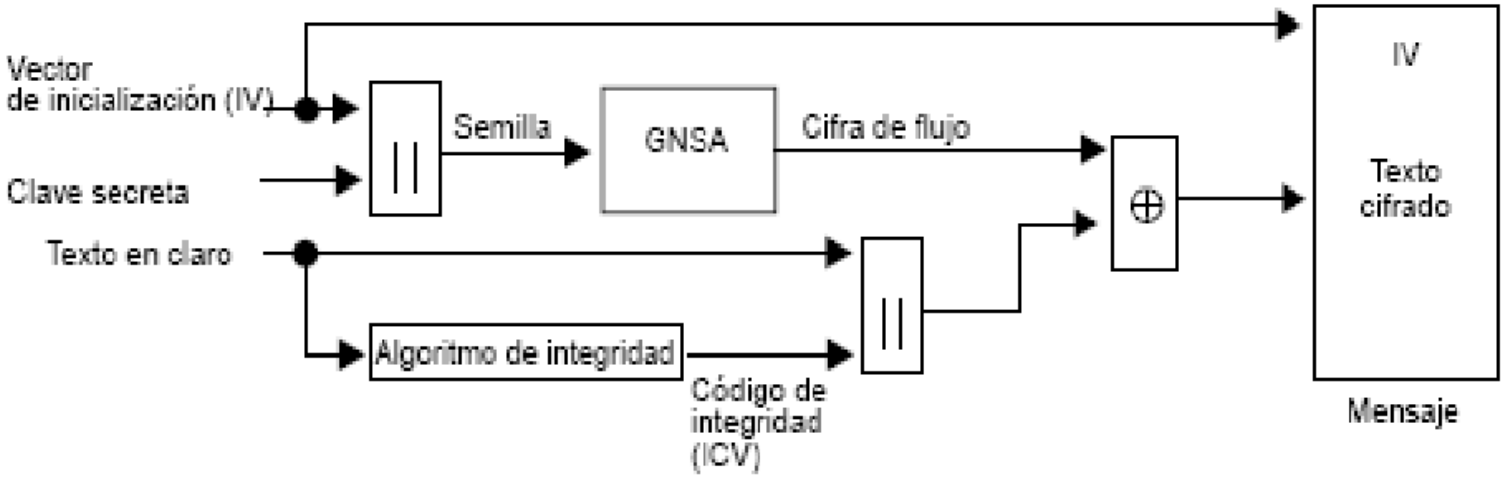
- Filtrado de direcciones MAC
- WEP (*Wired Equivalent Privacy*)
- WPA (*WI-FI Protected Access*)
- WPA 2
- 802.1x
- VPN (*Virtual Private Network*)

Filtrado de direcciones MAC

- Configurar en el punto de acceso las direcciones MAC (*Media Access Control*) de las tarjetas de red inalámbricas que se permiten
- Sencillo pero no es escalable
- Direcciones MAC viajan sin cifrar (*AirJack* o *WellenReiter*)

WEP (*Wired Equivalent Privacy*)

- Consiste en proteger los datos que se transmiten en una conexión inalámbrica mediante cifrado.
- Clave WEP estática y 24 bits de IV (WepCrack).
- Se recomienda utilizar WPA o WPA2.



WPA (*Wi-Fi Protected Access*)

- Es un estándar propuesto por los miembros de la Wi-Fi Alliance en colaboración con la IEEE.
- WPA propone un nuevo protocolo para cifrado, conocido como TKIP (*Temporary Key Integrity Protocol*).
- Emplea claves de 128 bits
- Este protocolo se encarga de cambiar la clave compartida entre punto de acceso y cliente cada cierto tiempo
- La integridad se usa con el código MIC basado en desplazamientos y sumas que no penalizan su rendimiento

WPA 2 (*Wi-Fi Protected Access 2*)

- Corrige las vulnerabilidades detectadas en WPA.
- Utiliza el algoritmo de cifrado AES.

VPN (*Virtual Private Network*)

- La red privada virtual emplea tecnologías de cifrado para crear un canal virtual privado sobre una red de uso público.
- Se emplean protocolos de encapsulamiento o *tunneling* que cifran y encapsulan los paquetes de datos: PPTP, L2F y L2TP