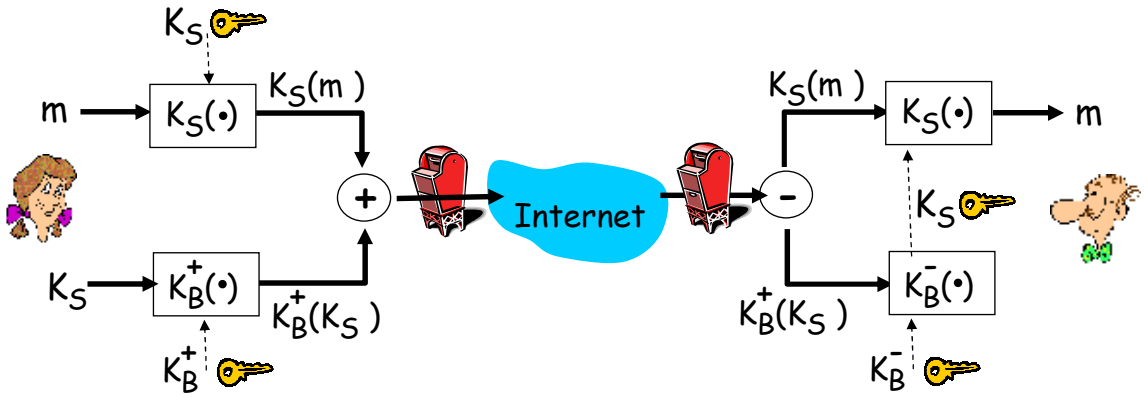
Capítulo 8: Agenda

8.1 ¿Qué es seguridad en red?
8.2 Principios de la criptografía
8.3 Integridad de los mensajes
8.4 Autenticación del *end point*
8.5 E-mail seguro
8.6 Asegurando las conexiones TCP: SSL
8.7 Seguridad en la capa de red: IPsec
8.8 Asegurando las redes LAN inalámbricas
8.9 Seguridad Operacional: *firewalls* e IDS

e-mail seguro

- Alice quiere enviar un e-mail confidencial, **m**, a Bob.

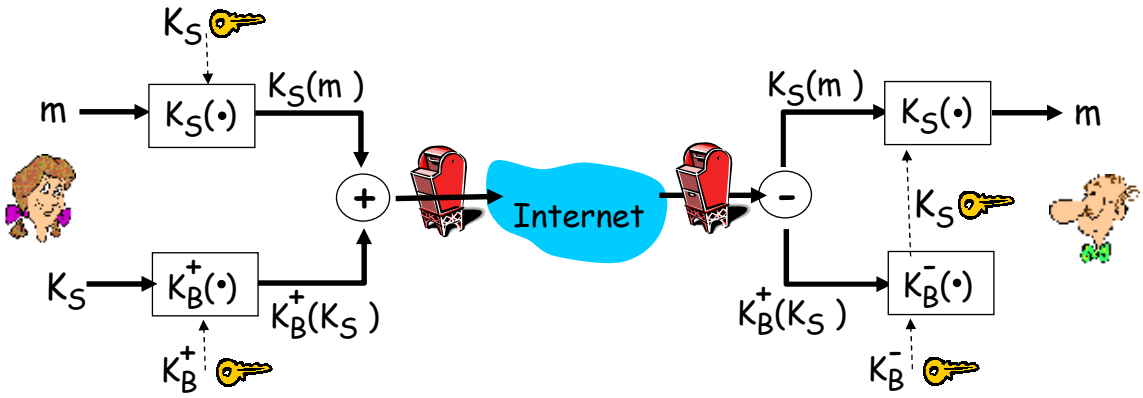


Alice:

- genera una clave privada *simétrica* randómica, K_S.
- cifra el mensaje con K_S (por eficiencia).
- además cifra K_S con la clave pública de Bob.
- envía ambas cosas, $K_S(m)$ y $K_B^+(K_S)$ a Bob.

e-mail seguro

- Alice quiere enviar un e-mail confidencial, m, a Bob.

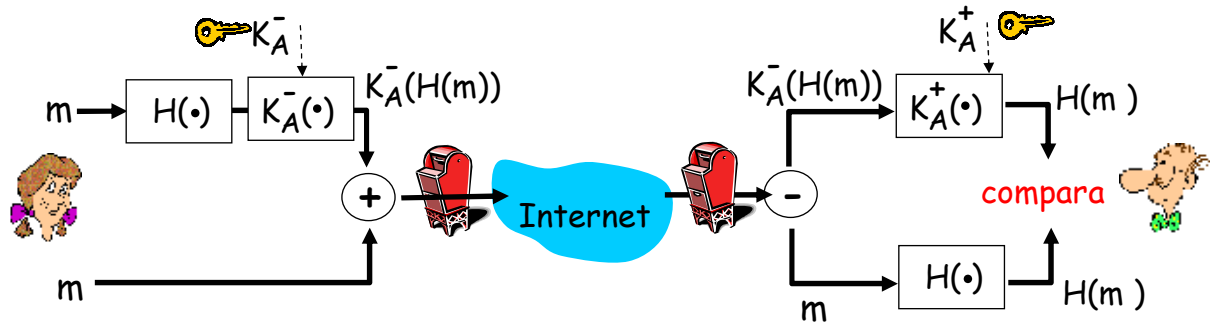


Bob:

- utiliza su clave privada para descifrar y recuperar K_S
- utiliza K_S para descifrar $K_S(m)$ y recuperar m

e-mail seguro

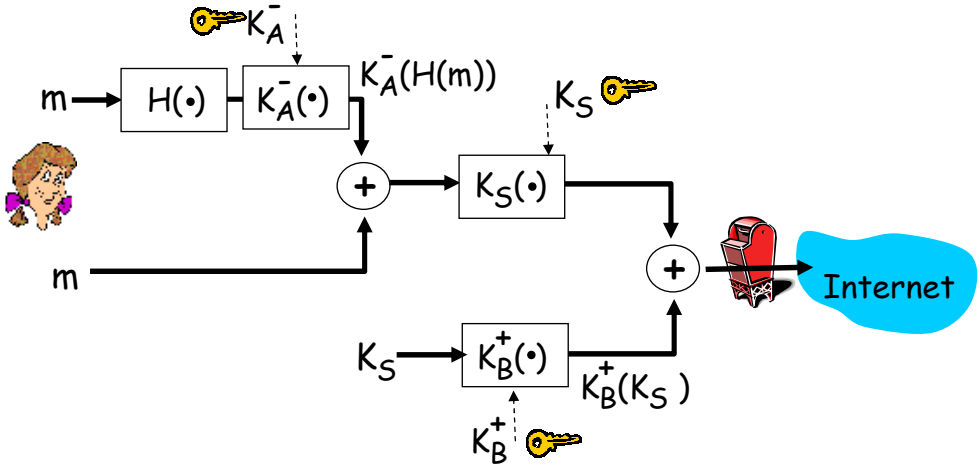
• Alice quiere brindar <u>autenticación de origen</u> e <u>integridad</u> al mensaje.



• Alice firma digitalmente un hash del mensaje.
• envía ambos, el mensaje (en texto claro) y la firma digital.

e-mail seguro

- Alice quiere brindar confidencialidad, autenticación de origen e integridad del mensaje.



Alice utiliza tres claves: su clave privada, la clave pública de Bob y la recientemente creada clave simétrica (*session key*: *one-time key*)

Pretty Good Privacy (PGP)

- 1991
- Esquema de cifrado de e-mail en Internet; estándar de-facto.
- Utiliza criptografía de clave simétrica, de clave pública, función de hash y firma digital.
- brinda secreto, autenticación de origen e integridad.
- *Web of trust.*
- Inventor: Phil Zimmerman; investigador investigado durante varios años.

Un mensaje firmado con PGP:

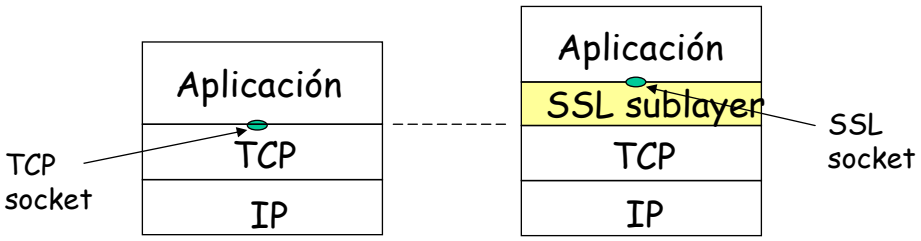
```
---BEGIN PGP SIGNED
   MESSAGE---
Hash: SHA1

Bob:My husband is out of
   town tonight.Passionately
   yours, Alice

---BEGIN PGP SIGNATURE---
Version: PGP 5.0
Charset: noconv
yhHJRHhGJGhgg/12EpJ+lo8gE4v
   B3mqJhFEvZP9t6n7G6m5Gw2
---END PGP SIGNATURE---
```

Capítulo 8: Agenda

8.1 ¿Qué es seguridad en red?
8.2 Principios de la criptografía
8.3 Integridad de los mensajes
8.4 Autenticación del *end point*
8.5 e-mail seguro
8.6 Asegurando las conexiones TCP: SSL
8.7 Seguridad en la capa de red: IPsec
8.8 Asegurando las redes LAN inalámbricas
8.9 Seguridad Operacional: *firewalls* e IDS

Secure Sockets Layer (SSL)

- Brinda seguridad en capa de transporte a cualquier aplicación basada en TCP.
  - p.e., entre browser y servidor web (https)
  - IETF: TLS (*Transport Layer Security*) – RFC 5246
- servicios de seguridad:
  - Autenticación del servidor, cifrado, integridad y autenticación del cliente (opcional)

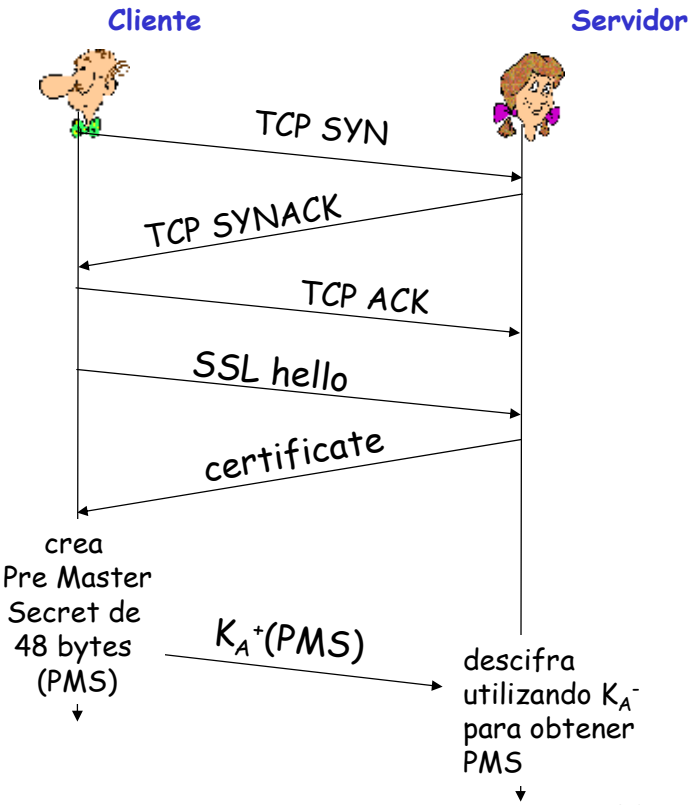


TCP TCP "enriquecido" con SSL

SSL: tres fases

1. Handshake:

- Bob establece una conexión TCP con Alice
- Bob autentica a Alice a través de un certificado firmado por una CA
- Bob crea, cifra (utilizando la clave pública de Alice), y envía la ***pre master secret key*** a Alice
  - El intercambio de ***nonce*** no se muestra



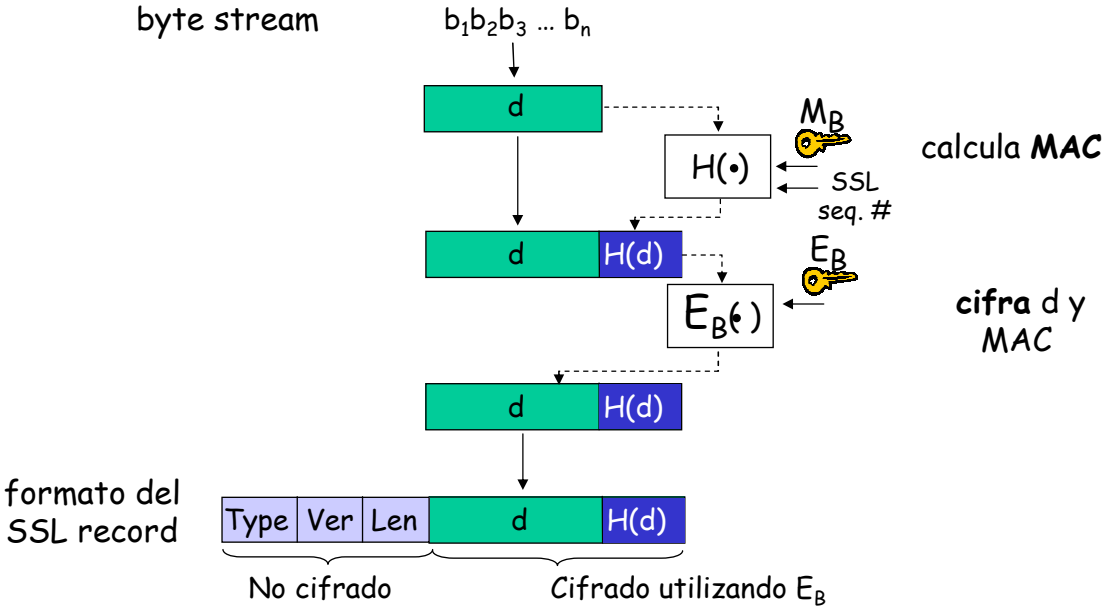
SSL: tres fases

2. Derivado de claves:

- A partir de la PMS y de los *nonces*, se calcula la MS
- Alice, Bob utilizan la *Master Secret* (MS) para generar 4 claves:
  - E_B: clave de cifrado de datos Bob -> Alice
  - E_A: clave de cifrado de datos Alice -> Bob
  - M_B: clave MAC Bob -> Alice
  - M_A: clave MAC Alice -> Bob
- Los algoritmos de **cifrado** y **MAC** son negociados entre Bob y Alice

SSL: tres fases

3. Transferencia de datos



Capítulo 8: Agenda

8.1 ¿Qué es seguridad en red?
8.2 Principios de la criptografía
8.3 Integridad de los mensajes
8.4 Autenticación del *end point*
8.5 e-mail seguro
8.6 Asegurando las conexiones TCP: SSL
8.7 Seguridad en la capa de red: IPsec
8.8 Asegurando las redes LAN inalámbricas
8.9 Seguridad Operacional: *firewalls* e IDS

IPsec: Seguridad en la Capa de Red

- IP Security
- Secreto en capa de red
  - el host que envía, cifra los datos en el datagrama IP
- Autenticación de capa de red
  - El host destino puede autenticar la dirección IP origen
- Dos protocolos principales:
  - Protocolos *Authentication Header* (**AH**)
  - Protocolo *Encapsulation Security Payload* (**ESP**)

- Se crea un canal lógico de capa de red (¡conexión en IP!) llamado *Security Association* (**SA**)
- cada SA es unidireccional (simplex)
- "Bundles" de SAs
- Puede tener un tiempo y/o tráfico de vida
- ID de conexión de 32 bits (**SPI**: ***S**ecurity **P**arameter **I**ndex*)

IPsec: Seguridad en la Capa de Red

- Hablando de seguridad, IPsec es un batallón de estándares
  - RFCs 2411, 4301, 4302, 4303, 4305, 4308, …
- Tercer protocolo involucrado
  - Establec. de SAs (acuerdo de algoritmos y claves)
    - **IKE**: Internet Key Exchange (RFC 2409)
    - También se puede hacer manualmente
- Tipos de dispositivos
  - *Hosts* y *Security Gateways*
- Modos de operación
  - Túnel y Transporte
- IPv4 e IPv6
- VPN: Redes Privadas Virtuales

Protocolo AH

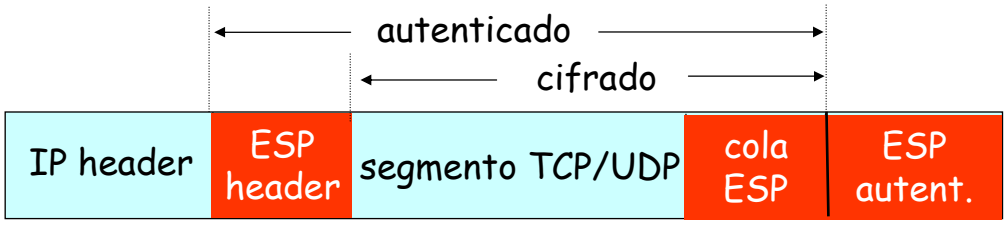
- brinda autenticación de origen, integridad pero no confidencialidad
- El encabezado AH se inserta entre el encabezado IP y el campo de datos.
- Campo protocolo: 51
- Los routers intermedios procesan el datagrama de la manera usual

El encabezado AH incluye:

- Identificador de conexión (SPI)
- Campo "próximo encabezado": especifica el tipo de datos que lleva (p.e., TCP, UDP, ICMP)
- Número de secuencia
- MAC del datagrama y del encabezado AH excepto algunos campos de ellos.

Protocolo ESP

- brinda confidencialidad, autenticación de origen e integridad de los datos.
- datos y cola ESP cifrados.
- El campo *next header* está en la cola del ESP.
- El campo de autenticación de ESP es similar al campo de autenticación de AH.
- Protocolo = 50.



Capítulo 8: Agenda

8.1 ¿Qué es seguridad en red?
8.2 Principios de la criptografía
8.3 Integridad de los mensajes
8.4 Autenticación del *end point*
8.5 e-mail seguro
8.6 Asegurando las conexiones TCP: SSL
8.7 Seguridad en la capa de red: IPsec
8.8 Asegurando las redes LAN inalámbricas
8.9 Seguridad Operacional: *firewalls* e IDS

Seguridad IEEE 802.11

- La frontera de la red es el alcance de la señal
- La comodidad no es muy amiga de la seguridad
- Sigue siendo relativamente común
  - no uso de cifrado y/o autenticación
  - *sniffing* de paquetes y varios ataques sencillos
- asegurando 802.11
  - cifrado, autenticación
  - el primer intento fue Wired Equivalent Privacy (WEP): falló
  - intento actual: 802.11i

Wired Equivalent Privacy (WEP):

- 1997
- autenticación
  - El *host* requiere autenticación del *access point*
  - El *access point* envía un *nonce*
  - El *host* cifra el *nonce* utilizando una clave secreta compartida
  - El *access point* descifra el *nonce* y así autentica al *host*
- no hay mecanismo de distribución de clave
- autenticación: conociendo la clave compartida es suficiente

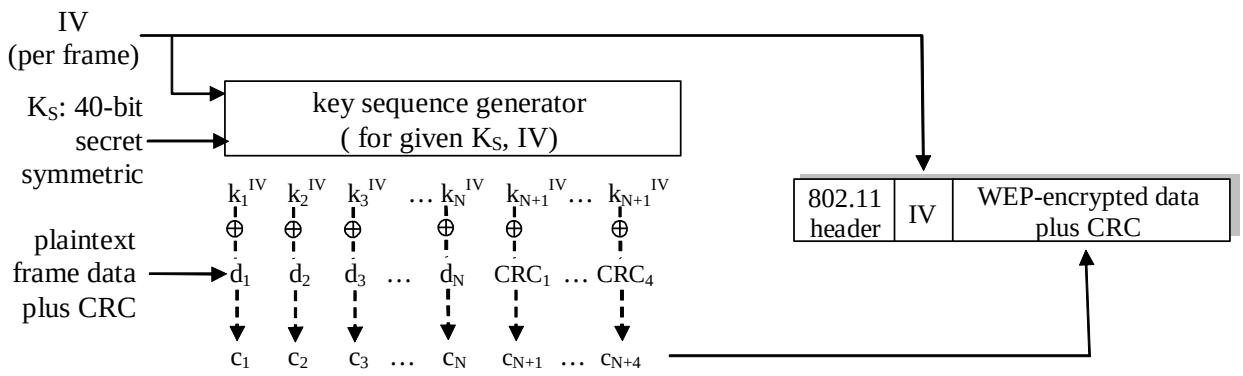
Cifrado de datos en WEP

- El *host* y el AP comparten una clave simétrica de 40 o 104 bits (semi-permanente)
- El host le agrega un vector de inicialización (IV) de 24 bits para crear una clave de 64 o 128 bits
- Esta clave es utilizada para generar un stream de claves, k_i^{IV}
  - Cifrado de flujo con algoritmo RC4
- k_i^{IV} es utilizada para cifrar el byte iésimo, d_i, en la trama:

$$c_i = d_i \text{ XOR } k_i^{IV}$$

- IV y los bytes cifrados c_i , son enviados en la trama

Cifrado WEP de 802.11

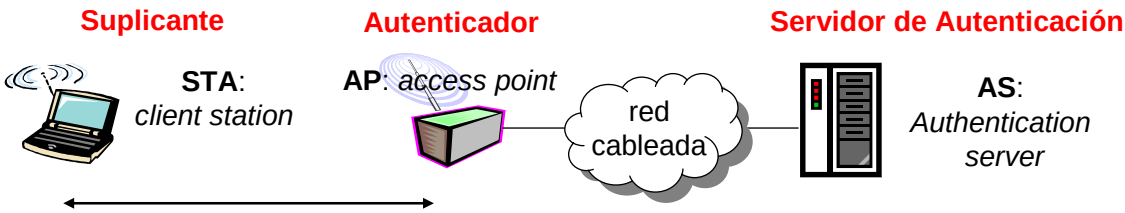


Cifrado WEP

802.11i: seguridad mejorada

- 2004
- numerosas (y más fuertes) formas posibles de cifrar y brindar integridad
- brinda distribución de claves
- utiliza un servidor de autenticación separado del *access point*
- WPA (*WiFi Protected Access*) o WPA2
- 802.1X: *Port Based Network Access Control*
  - *Wired* y *wireless*
- EAP: ***E**xtensible **A**uthentication **P**rotocol*
  - RFC 3748

802.11i: 4 fases de operación



1 **Descubrimiento** de prestaciones de seguridad

2 La STA (el usuario) y el AS se **autentican** (mutuamente), y generan la Master Key (**MK**). El AP oficia de "pasarela"

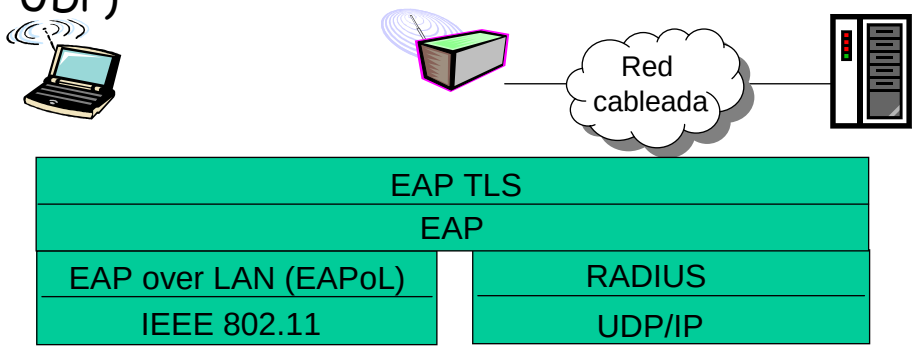
3 La STA deriva la Pairwise Master Key (**PMK**)

3 El AS deriva la misma PMK, y se la envía al AP

4 La STA y el AP utilizan la PMK para derivar la Temporal Key (**TK**) utilizada para cifrado e integridad de los mensajes

EAP: *Extensible Authentication Protocol*

- EAP: protocolo entre el cliente (móvil) y el servidor de autenticación
- EAP se envía sobre enlaces separados
  - Móvil -> AP (EAP over LAN)
  - AP -> servidor de autenticación (RADIUS sobre UDP)



Capítulo 8: Agenda

8.1 ¿Qué es seguridad en red?
8.2 Principios de la criptografía
8.3 Integridad de los mensajes
8.4 Autenticación del *end point*
8.5 e-mail seguro
8.6 Asegurando las conexiones TCP: SSL
8.7 Seguridad en la capa de red: IPsec
8.8 Asegurando las redes LAN inalámbricas
8.9 Seguridad Operacional: *firewalls* e IDS

Internet…

- … es un lugar inseguro

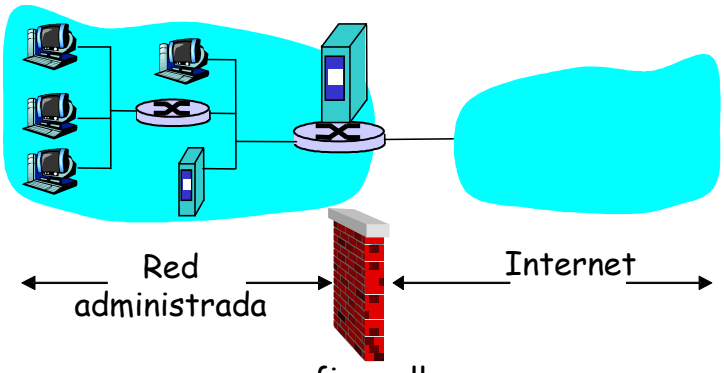
- Control de acceso
- Control de salida

- Algunas soluciones (paliativos) disponibles:
  - Firewalls
  - IDS
  - IPS

Firewalls

firewall

Aisla la red interna de la organización de Internet, permitiendo que algunos paquetes pasen y que otros sean bloqueados.



Configuración más básica

Firewalls

- Hardware y/o software
- Definen fronteras entre redes
- Tenemos una política de seguridad de la red que en la frontera es la "seguridad perimetral"
- Debemos
  - configurarlos adecuadamente para evitar tener una sensación falsa de seguridad
  - registrar su actividad y analizarla
  - No deben haber caminos alternativos
- El propio firewall debe estar protegido del acceso a él
- No sólo debemos proteger nuestra red de Internet, también debemos proteger a Internet de nuestra red

Firewalls

- En general, tres zonas

Tres tipos de firewalls:

- *stateless packet filters* (los tradicionales, "la primera generación")
- *stateful packet filters*
- *application gateways o application proxy*

Stateless packet filtering

- Red interna conectada a Internet a través de un (router) firewall
- router filtra paquete por paquete, la decisión para *forward/drop* del paquete se basa en "mirar" cosas como:
  - Dirección IP origen, dirección IP destino
  - Números de puertos origen y destino TCP/UDP
  - Tipo de mensaje ICMP
  - Campo "protocolo" de IP
  - Flags de TCP: SYN, ACK, …
  - Interfaz
  - …

Incluso combinándolas

Stateless packet filtering: ejemplos

- Ejemplo 1: bloquear los datagramas entrantes y salientes con el campo protocolo = 17 y con puerto origen o destino = 23.
  - Todos los flujos entrantes y salientes UDP de conexiones telnet son bloqueadas.
- Ejemplo 2: bloquear segmentos TCP entrantes con ACK=0.
  - Previene que clientes externos hagan conexiones TCP con clientes internos, pero permite que clientes internos se conecten hacia afuera.
- Ejemplo 3: rangos de direcciones IP privadas
- Ejemplo 4: "filtros *antispoofing*"

Stateless packet filtering: más ejemplos

Política	Configuración del Firewall
No acceso a Web externo.	*Drop* de todos los paquetes salientes a cualquier dirección IP, puerto 80
No conexiones TCP entrantes, excepto aquellas para el servidor Web público.	*Drop* de todos los paquetes TCP SYN entrantes hacia cualquier IP excepto *dir_IP_servidor_web*, puerto 80
Prevenir que el tráfico UDP "ruidoso" consuma todo el ancho de banda disponible.	*Drop* de todos los paquetes UDP entrantes - excepto DNS.
Prevenir que se pueda realizar traceroute a su red	*Drop* de todo el tráfico ICMP "TTL expirado" que intente abandonar la red administrada

Access Control Lists

- *ACL:* tabla de reglas, aplicada de arriba hacia abajo a paquetes entrantes: parejas (acción, condición)

action	source address	dest address	protocol	source port	dest port	flag bit
allow	222.22/16	outside of 222.22/16	TCP	> 1023	80	any
allow	outside of 222.22/16	222.22/16	TCP	80	> 1023	ACK
allow	222.22/16	outside of 222.22/16	UDP	> 1023	53	---
allow	outside of 222.22/16	222.22/16	UDP	53	> 1023	----
deny	all	all	all	all	all	all

Stateful packet filtering

- stateless packet filter: herramienta con poco "margen de maniobra"
  - admite paquetes que "no tienen sentido," p.e., source port = 80, ACK bit set, aún cuando no hay una conexión TCP establecida

action	source address	dest address	protocol	source port	dest port	flag bit
allow	outside of 222.22/16	222.22/16	TCP	80	> 1023	ACK

- *stateful packet filter:* sigue el estado de cada conexión TCP
  - sigue el establecimiento de la conexión (SYN), la liberación (FIN): puede determinar cuando los paquetes entrantes y salientes "tienen sentido"
  - *timeout* de conexiones inactivas en el *firewall*: no se admiten más paquetes

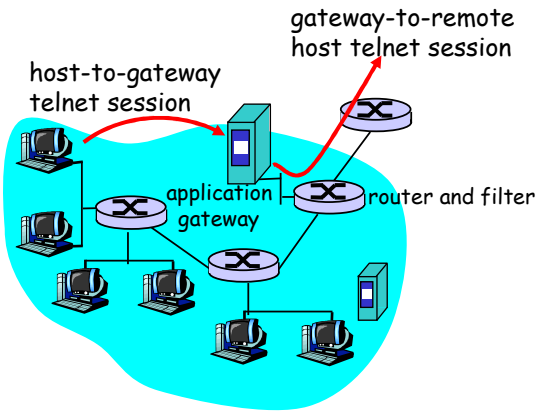
Stateful packet filtering

- ACL ampliada para indicar la necesidad de chequear el estado de la conexión antes de admitir un paquete

action	source address	dest address	proto	source port	dest port	flag bit	check conexion
allow	222.22/16	outside of 222.22/16	TCP	> 1023	80	any	
allow	outside of 222.22/16	222.22/16	TCP	80	> 1023	ACK	X
allow	222.22/16	outside of 222.22/16	UDP	> 1023	53	---	
allow	outside of 222.22/16	222.22/16	UDP	53	> 1023	----	X
deny	all	all	all	all	all	all	

Application gateways

- filtran paquetes en base a los datos de aplicación, además de los campos de IP/TCP/UDP…
- ejemplo: permitir sólo a un grupo de usuarios internos, realizar telnet al exterior.



1. requiere a todos los usuarios a hacer telnet a través del gateway.
2. para los usuarios autorizados, el gateway establece una conexión telnet con el host destino. El gateway hace relay de los datos entre las dos conexiones
3. Los filtros del router bloquean todas las conexiones telnet no originadas desde el gateway.

Limitaciones de los firewalls y gateways

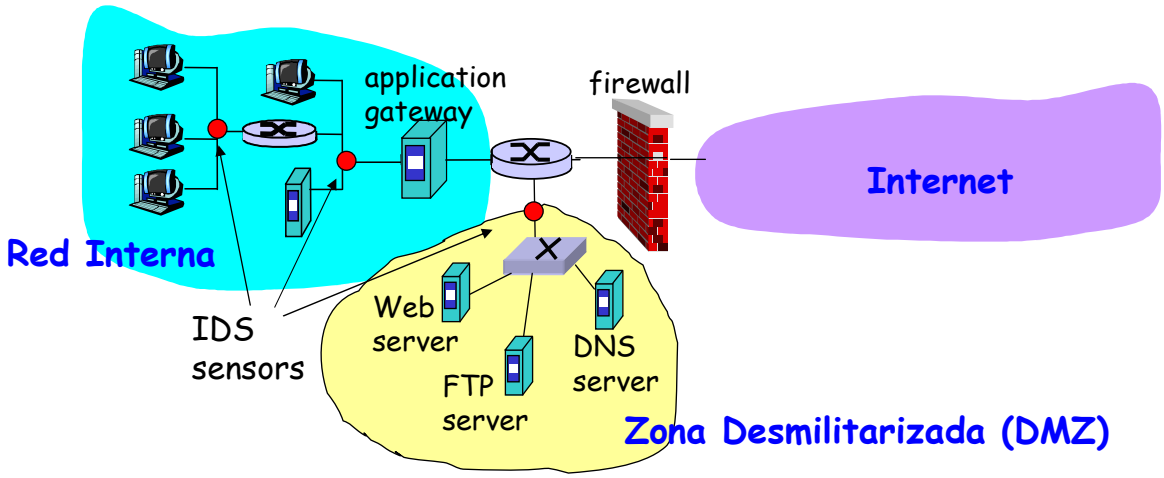
- IP *spoofing*: el router no puede saber si los datos provienen del origen mencionado
- Si varias aplicaciones requieren un tratamiento especial, cada una requiere su propio *app. gateway*.
- El software del cliente debe conocer cómo contactar al gateway.
  - p.e., debe config. la dir. IP del proxy en el Web browser

Intrusion Detection Systems

- Filtrado de paquetes
  - opera solamente en los encabezados TCP/IP
  - no hay chequeos correlacionados entre sesiones
- *IDS: Intrusion Detection System*
  - *deep packet inspection:* observa el contenido del paquete (p.e., chequea strings de caracteres en el paquete contra una base de datos de patrones o expresiones conocidos por "sospechosos")
  - examina correlación entre múltiples paquetes
    - *port scanning, network mapping, DoS attack*
  - Genera alertas al detectar tráfico sospechoso

Intrusion Detection Systems

- múltiples IDSs: diferentes tipos de chequeos en diferentes lugares



Intrusion "X" Systems

*IPS: **I**ntrusion **P**revention **S**ystem*

- dispositivo que toma acciones frente a un tráfico sospechoso
  - Agrega un filtro en un firewall
  - Aumenta el nivel de *logging*
  - Cierra conexiones
  - …

- Falsos positivos y falsos negativos
- Sistemas basados en
  - firmas o "signatures"
  - anomalías

Basados en firmas

- Contienen una base de datos de firmas que debe estar siempre actualizada
  - Firma: es un comportamiento (tráfico) que significa una actividad sospechosa (posible intrusión)
  - Limitantes
    - Se debe conocer el ataque
    - El sistema debe estar actualizado
    - Falsos positivos y falsos negativos

Basados en anomalías

- Sistemas basados en anomalías
  - Hay una fase de aprendizaje del "tráfico normal" y luego, actúa en función del apartamiento del mismo. Esto se puede (debe) repetir
  - Limitantes
    - ¿Qué es normal?
    - ¿Qué es anormal?
    - Falsos positivos y falsos negativos

Seguridad en la red (resumen)

Técnicas básicas……

- criptografía (simétrica y pública)
- integridad de los mensajes
- autenticación del *end-point*

…. utilizadas en diferentes escenarios

- e-mail seguro
- transporte seguro (SSL)
- IPsec
- 802.11

Seguridad operacional: firewalls e I"x"S

Fin del teórico 2009