GRUPO DE SEGURIDAD INFORMÁTICA

Problemas de Seguridad en Redes TCP/IP

Capa 3 en internet

- IPv4 e IPv6
- Muy similares en sus características de seguridad
- IPSec es obligatorio (de implementar) en IPv6
- Servicio de datagramas. No hay garantías de entrega/duplicados/retardos. No hay garantías de origen
  - Cualquier equipo puede enviar un paquete con IP de origen arbitraria
  - Algunos proveedores filtran, otros no

IP

- Salvo en ambientes muy controlados, no puede garantizarse la relación IP <-> máquina
  - En Internet, ni siquiera IP <-> empresa
- Es muy difícil rastrear un ataque proveniente de Internet con direcciones origen modificadas

Interacción de IP y la capa MAC

- ARP - Mapeo de dirección de capa 3 a dirección de capa MAC
- Protocolo muy sencillo.
  - A envía consulta por Broadcast pidiendo MAC correspondiente a la IP B
  - "B" responde
- Cualquiera puede responder
- Idea: modificar el mapeo en cache

ARP spoofing

- La mayoría de los sistemas aceptan respuestas a preguntas que no hicieron, o actualizan su cache ante un pedido
- Si lo “refresco” suficientemente seguido, no hará un nuevo pedido broadcast
- Permite ataques Man In The Middle, escuchas, Negación de servicio, etc.
- Es lo que se utilizó en el primer laboratorio

ARP Spoofing "Soluciones"

- Configuración de entradas ARP estáticas
- Separación de redes críticas
- Monitoreo de cambios en las entradas de ARP
- Encriptación en capas superiores
- Algunos equipos, al recibir un ARP donde cambia un mapeo existente IP-MAC, mandan una consulta ARP a la vieja MAC. Solo funciona si la entrada aún está en cache

Otros problemas en capa 3

- **Ataques** a los protocolos de **ruteo**
  - Si puedo modificar la información de ruteo, puedo encaminar tráfico importante por donde no debería
  - Es común que los protocolos de ruteo interno se ejecuten sin medidas de seguridad (aunque estas estén disponibles)
  - Con ruteo externo (BGP), el mayor peligro son publicaciones a través de proveedores que no filtren adecuadamente a sus clientes
- Ataques con paquetes de control (**ICMP**)

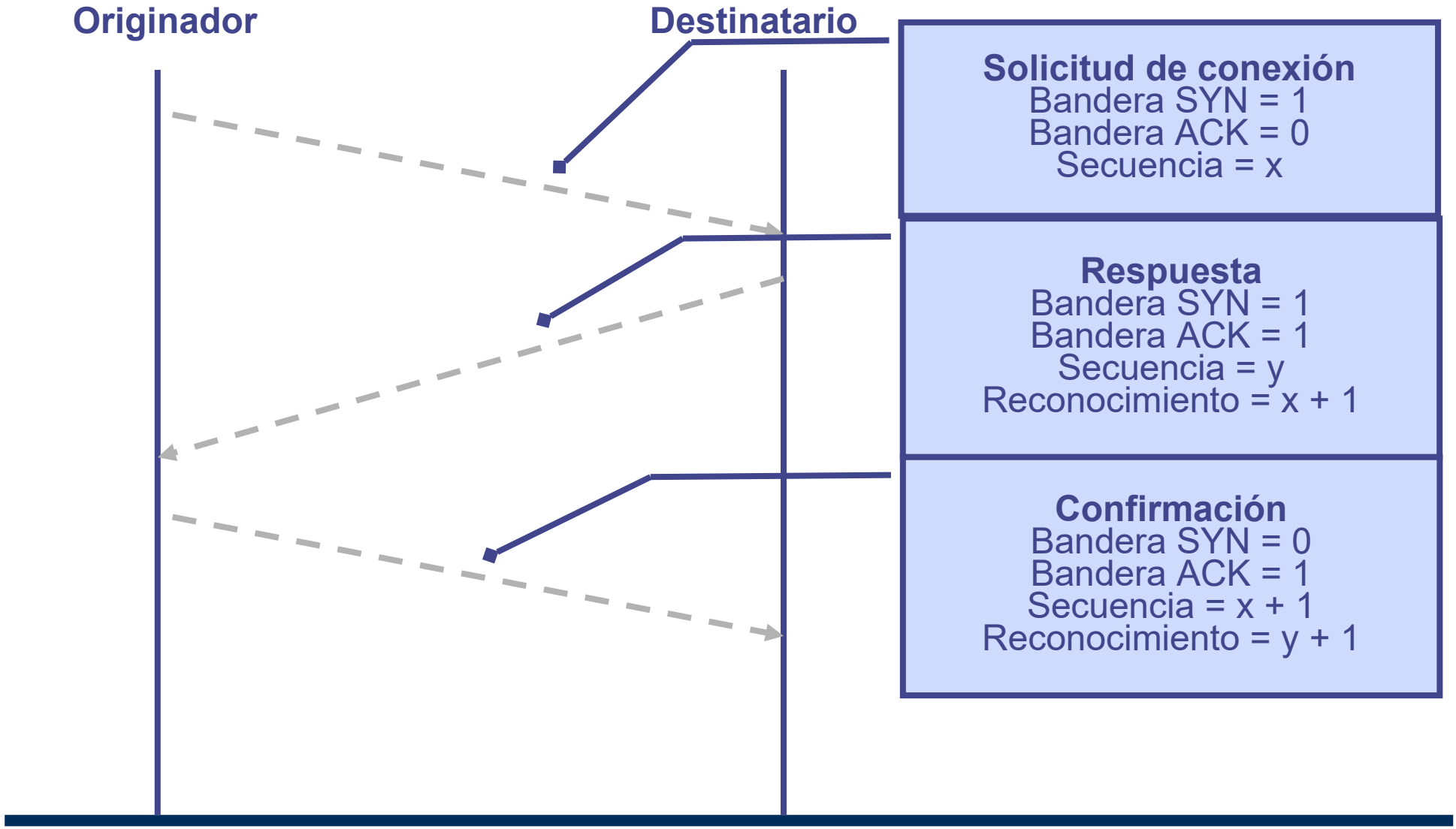
Capa 4 en internet

- UDP (servicio de datagrama): junto con IP, muy fácil hacer spoofing de solicitudes (ej. DNS)
- Muy difícil distinguir solicitudes válidas de inválidas. No hay estado en las solicitudes

TCP

- Orientado a conexión, confiable
  - Número de secuencia para detectar segmentos duplicados, faltantes, reordenados, fuera de secuencia
  - Suma de comprobación para detectar errores de transmisión
  - No sirve para detectar modificación maliciosa
- Establecimiento de conexión de 3 vías

Establecimiento de conexión en TCP



Establecimiento de conexión en TCP

- Si yo quiero insertar datos en una conexión, debo conocer:
  - puertos origen y destino
  - IP origen y destino
  - Números de secuencia dentro de la ventana del receptor
- Idem para establecer una conexión “a ciegas”
- El número de secuencia inicial se elije “aleatoriamente”, no solo en base a un reloj como se hizo inicialmente

TCP sesion hijacking

$C \rightarrow S: SYN(ISN_C)$

$S \rightarrow C: SYN(\mathbf{ISN_S}), ACK(ISN_C)$

$C \rightarrow S: ACK(ISN_S)$

$C \rightarrow S$:data and / or $S \rightarrow C$:data

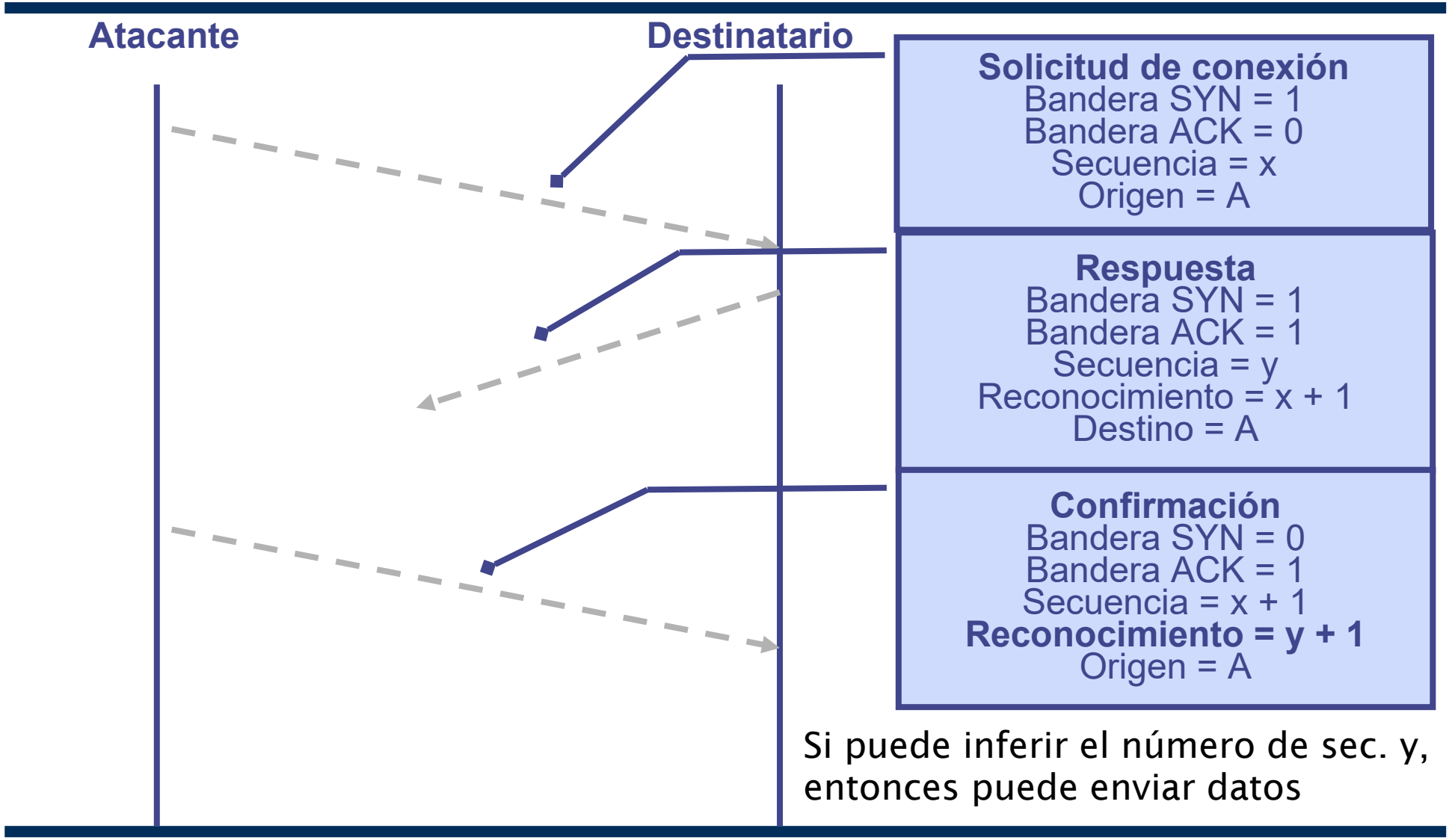
$X \rightarrow S: SYN(ISN_X)$,SRC = T

$S \rightarrow T: SYN(ISN_S)$,$ACK(ISN_X)$

$X \rightarrow S: ACK(\mathbf{ISN_S})$,SRC = T

$X \rightarrow S: ACK(ISN_S)$,SRC = T, nasty – data

TCP Session Hijacking



Algunas debilidades

- Por cada conexión, se debe guardar estado (incluso antes de completarse)
  - Syn flood: inundación de paquetes de establecimiento de conexión. Se ocupan recursos en conexiones que nunca se terminarán de establecer. Hay paliativos
  - Llenado de la tabla de conexiones establecidas
- Ataques con TCP reset (DOS)
- Ataques con ICMP unreachable
- Ataques con ICMP must-fragment

Capa de aplicación

- Donde se encuentran los servicios que le interesan al usuario
- Miles de potenciales servicios
  - Muchos de ellos sin ninguna consideración por la seguridad en su diseño
  - Otros mal implementados
- Algunos servicios se consideran parte de la infraestructura
  - DNS

Capa de aplicación

- Para conectarse a un determinado servicio, se utiliza el puerto de capa de transporte del mismo
  - Servicios bien conocidos. Ejemplos: http(80), smtp(25), pop3(110), ntp(123), dns (53), etc.
  - Otros. Pueden tener puertos fijos o algún servicio de directorio
- Portscan: búsqueda de servicios abiertos en una dirección o rango de direcciones
  - Intento de conexión a muchos puertos

DNS

- Resolución de nombres
- Sistema distribuido
  - Zonas de autoridad, con sus servidores autoritativos
  - Servidores recursivos que guardan cache
- Las consultas utilizan UDP
- 13 servidores “raiz” (13 direcciones IP), necesarios para comenzar cualquier búsqueda

Por qué es crítico

- Si no funciona, la mayoría de los servicios serían inalcanzables por la mayoría de los usuarios
- Si se modifican datos maliciosamente, se puede redirigir tráfico de un sitio legítimo o negar servicio
  - Phishing y otros ataques

Problemas del DNS

- Bugs de seguridad en servidores desactualizados (BIND estándar de facto)
- Cache corruption: ante una pregunta, el servidor devuelve datos relevantes para otra consulta, falsos. Versiones viejas de servidores recursivos caían en esta trampa
- No hay ninguna autenticación de las respuestas
- Bugs en los clientes
  - Aceptar respuestas a consultas que no se hicieron

Problemas del DNS

- Puede brindar información sobre los servicios brindados externamente (e internamente si los ponemos en el DNS)
  - Es común utilizar “split dns” (visiones distintas según desde donde o a qué servidor consultemos)
- Separar servidores internos (recursivos) de los externos, para evitar intentos de cache poisoning desde afuera
- Problemas de seguridad en los registros de nombres de dominio

Otras aplicaciones

- Cualquier aplicación accesible a través de una red es susceptible de ser atacada si tiene bugs en su implementación
- Históricamente, la cantidad de bugs de seguridad en servidores de todo tipo es alta
- A veces nos olvidamos que, por ejemplo, una impresora con conexión de red es tan vulnerable como nuestros servidores
- Algunos ejemplos se verán la semana que viene

Ataques comunes en redes

- Pruebas y escaneos: intentos de obtener información de sistemas remotos. Típicamente como precursores de futuros ataques
- Envío de paquetes que exploten vulnerabilidades en las implementaciones de los protocolos o las aplicaciones
- Captura de paquetes (packet sniffing) – capturar paquetes que pasan por la red y obtener información sensible

Otros tipos de ataques

- Negación de servicio (denial of service) – generar peticiones que carguen excesivamente o hagan colapsar un equipo o enlace
- Spoofing – hacerse pasar por otra máquina (u otro usuario)

Portscans

- Típicamente ataque “de reconocimiento”
- Búsqueda de servicios disponibles
- Detección de versiones
- “Fingerprint” del Sistema Operativo, parches

Ataques de negación de servicios

- Hemos visto que pueden ser causados por problemas en varias capas
  - ARP spoofing
  - Ataques a los protocolos de ruteo
  - Llenado de tablas de información de conexiones
  - Modificación de entradas en el DNS

Bibliografía y referencias

- **A. Tanenbaum.** *Redes de Computadoras.* 4Ta ed. Prentice Hall, 2003.
- **R. Anderson**, *Security Engineering – A Guide to Building Dependable Distributed Systems*, Wiley, 2001.
- **D. Gollman**, *Computer Security*, Wiley, 2006.