Seguridad en Internet
(2ª Sesión)

Jordi Forné

Universitat Politècnica de Catalunya

Escola Tècnica Superior d'Enginyeria de Telecomunicació de Barcelona

Departament de Matemàtica Aplicada i Telemàtica

UPC

DMAT

Prestaciones para el Atacante

Ataques	Prestaciones
Intercepción Escucha Análisis de tráfico	 Obtención de información privada Información sobre relaciones entre clientes
Suplantación	Mejora del perfil Fabricación de mensajes
Manipulación	Modificar, retrasar o eliminar mensajes
Intrusión	Acceso a recursos reservados
Degradación	Pérdida competitividad corporación

Seguridad

Amenaza + Vulnerabilidad = Ataque => Impacto

Identificar	Minimizar	Reducir y Detectar	Acotar

Problemática actual.

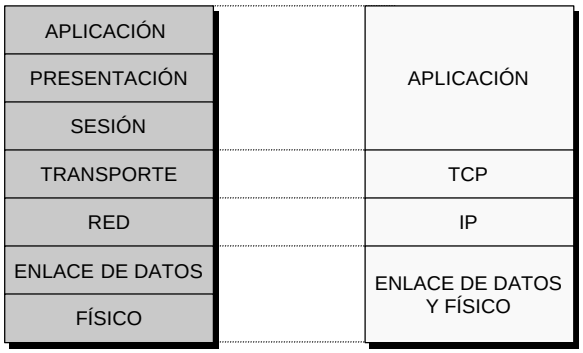
- Internet se ha convertido en el medio más popular de interconexión de recursos informáticos.
- Se utilizan las redes IP para la transmisión de información crítica.
- Mayor facilidad para realizar un ataque al disponer de tecnología más sofisticada.

Solución.

- Implantación de Servicios de Seguridad para proteger la comunicación:
  - Privacidad.
  - Autenticidad.
  - Verificabilidad.

Ubicación de los Servicios de Seguridad.

Equivalencia entre los modelos OSI y TCP/IP.



Ubicación de la Seguridad en el nivel de Aplicación (I).

- Solución adecuada si:
  - El servicio de seguridad es específico de la aplicación.
  - El servicio de seguridad pasa a través de aplicaciones intermedias.

Ejemplo: SSH, SET, PGP y S/MIME

Ubicación de la Seguridad en el nivel de Aplicación (II).

- Ventajas:
  - Menos datos a procesar.
  - Interfaz sencilla con la aplicación.
  - Compatibilidad con sistemas conectados a otro tipo de redes.
- Desventajas:
  - Implementación para cada aplicación en cada sistema extremo.
  - No se protegen las cabeceras de los protocolos de nivel inferior.

Ubicación de la Seguridad por debajo del nivel de Aplicación (I).

Niveles TCP/IP

- Los datos procedentes de la aplicación se cifran en el terminal origen antes de ser transmitidos

Ejemplo: SSL, TLS, WTLS

Ubicación de la Seguridad por debajo del nivel de Aplicación (II).

- Ventajas:
  - Sólo es necesario diseñar dos interfaces entre el nivel de seguridad y el de transporte.
- Desventajas:
  - No se protegen las cabeceras de los protocolos de nivel inferior.
  - No permite ofrecer servicios a campos específico de la aplicación

Ubicación de la Seguridad por debajo del nivel TCP (I).

Niveles TCP/IP

- Suponer que los sistemas extremos son fiables y las redes subyacentes no.

Ejemplo: IPSEC

Ubicación de la Seguridad por debajo del nivel TCP (II).

- Ventajas:
  - Servicios de seguridad transparentes a las aplicaciones.
  - Protección de las cabeceras de los protocolos de las capas superiores.
  - La capa TCP cifrada oculta detalles de la red.
- Desventajas:
  - Compatibilidad con sistemas conectados a otro tipo de redes.

Ubicación de la Seguridad por debajo del nivel IP.

Niveles TCP/IP

- Si el descifrado de la cabecera IP no se realiza correctamente, los datos no llegarán a su destino.
- Todas las cabeceras se transmiten cifradas.
- Precisa confianza en nodos intermedios.

Política de Seguridad

Definición

- Conjunto de reglas que delimitan o controlan las actividades relevantes en cuanto a seguridad de sujetos o entidades.
- Política de seguridad
  - Estándares y reglas
  - Contratos de usuario
  - Procedimientos

Características

- Duración: 5 años
- Documento breve: 4 ó 5 planes
- Exige el compromiso de los usuarios
- No debe tener referencias a tecnología

Gestión de riesgos

- Coste asociado a los riesgos, en función de su probabilidad
- Coste asociado a las medidas de seguridad
- Gestión de riesgos: equilibrio entre coste protección y exposición
- Decisiones:
  - Aceptar riesgos
  - Asignarlos a terceros
  - Evitarlos

Implementación

- Medidas transparentes a usuarios
- Fomentar cultura de seguridad entre usuarios
- Todo bien determinado en la política de seguridad

Auditoría

- Automatización procesos cuando sea posible
- Programas fiables, scripts propios,...
- Monitorización del nivel de uso del sistema (root, usuarios, …)
- Recogida Logs del sistema