

Criptografía y Seguridad de Datos

Introducción

Carlos Figueira

Universidad Simón Bolívar

Basado en láminas del Prof Henric Johnson

(www.its.bth.se/staff/hjo/)

Contenido

- Sobre el curso
- Ataques, servicios y mecanismos
- Ataques de Seguridad
- Servicios de Seguridad
- Métodos de defensa
- Modelo para Seguridad en Redes
- Estándares

Sobre el curso

- Principios técnicos para proveer servicios de seguridad en redes
- Experiencias prácticas
- Programa

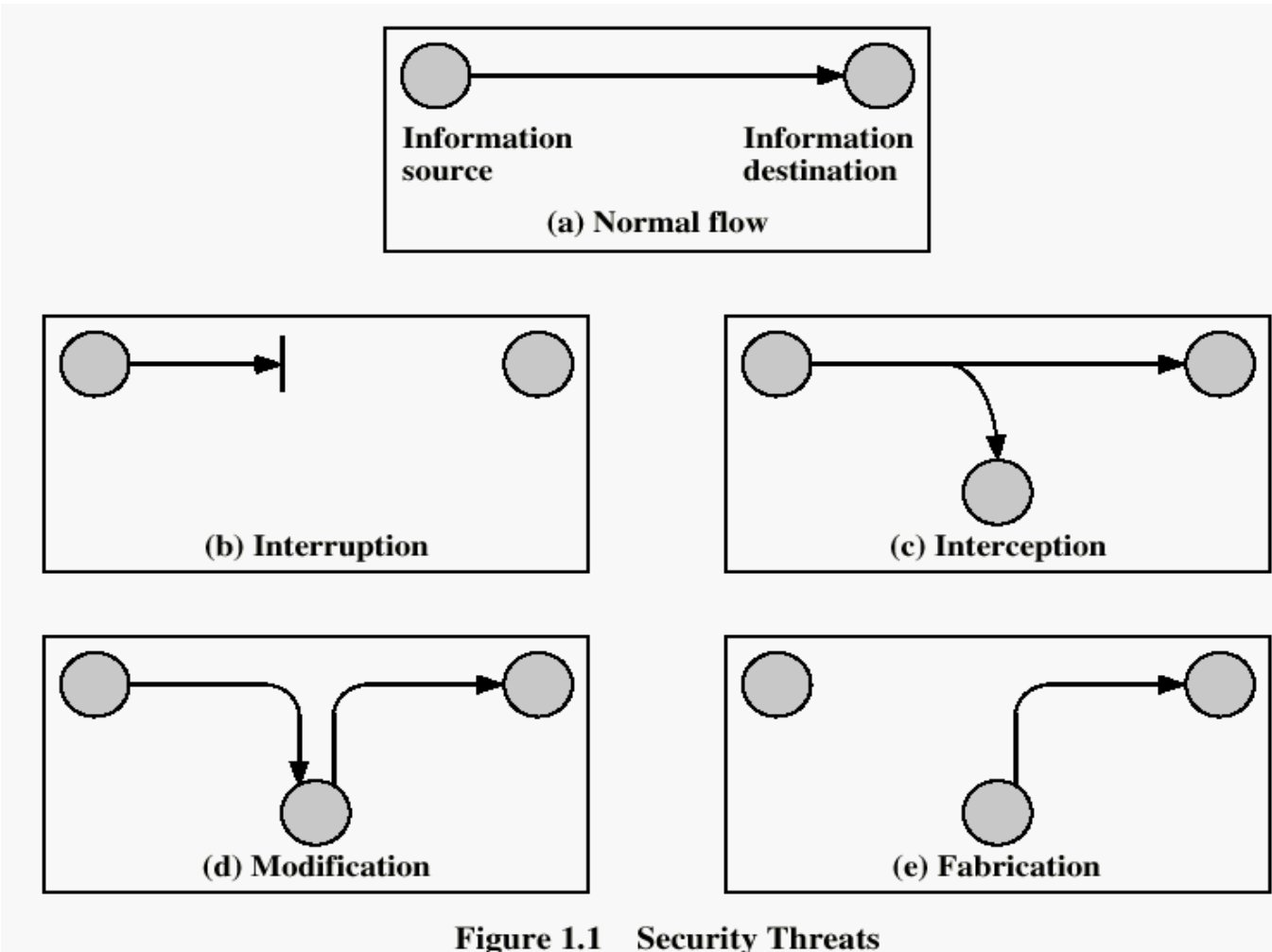
NO INCLUYE

- *Políticas, estándares seguridad de la información en organizaciones*
- *Curso práctico de “hacking ético”*

Definiciones

- **Ataques de Seguridad:** *cualquier acción que comprometa la seguridad de la info.*
- **Mecanismo de seguridad:** *mecanismo diseñado para detectar, prevenir o recuperarse de un ataque de seguridad.*
- **Servicio de Seguridad:** *Mejora seguridad de un sistema de procesamiento o transmisión de información. Utiliza 1 o más mecanismos de seguridad.*

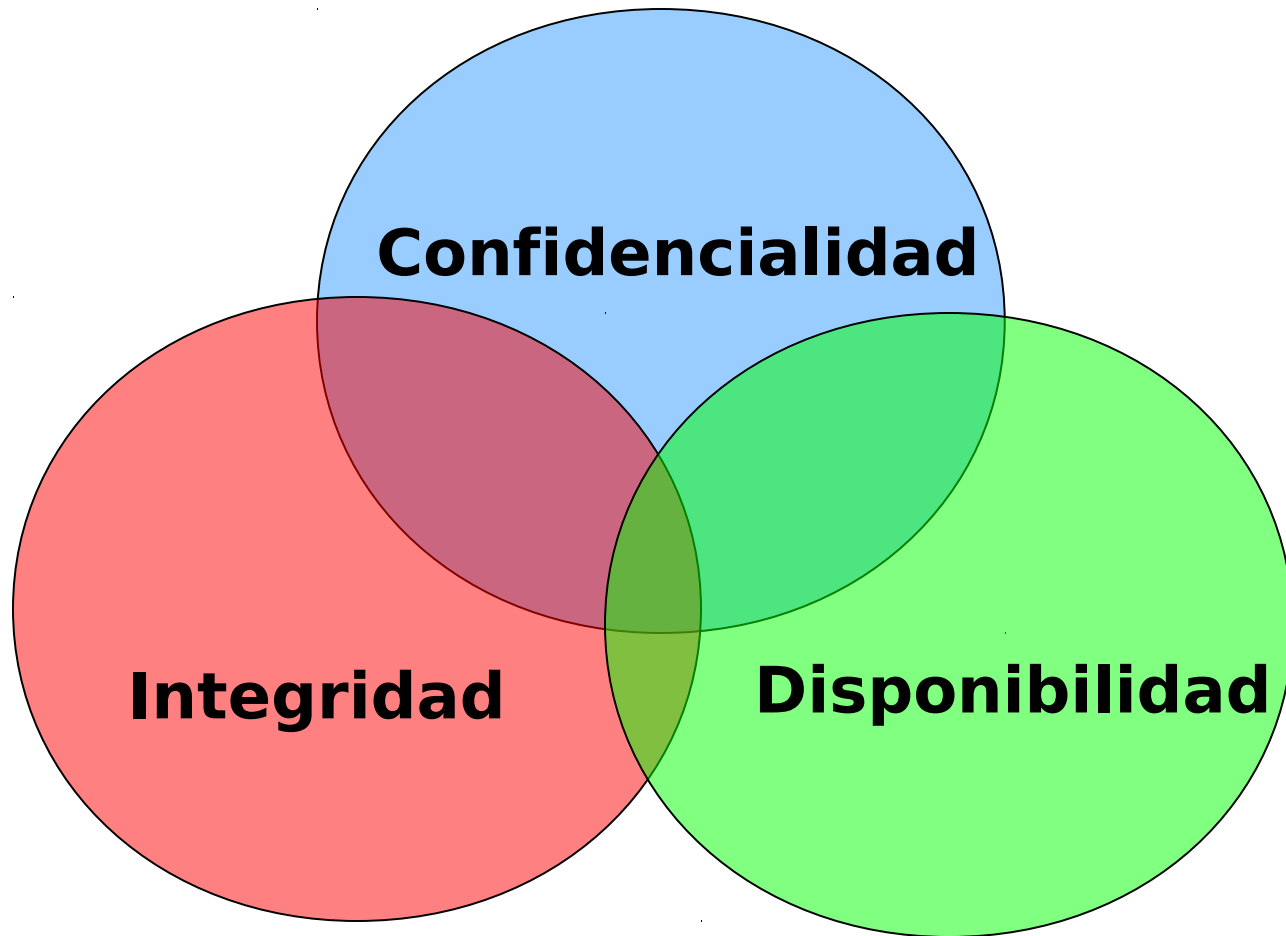
Ataques de seguridad



Ataques de Seguridad

- **Interrupción:** Ataque a la disponibilidad
- **Intercepción:** Ataque a la confidencialidad
- **Modificación:** Ataque a la integridad
- **Fabricación:** Ataque a la autenticidad

Objetivos de Seguridad



Tipos de ataques

- Pasivos:
 - Acceso a contenido de mensajes
 - Análisis de tráfico
- Activos:
 - Suplantación de identidad
 - Repetición
 - Modificación
 - Negación de servicio

Servicios de Seguridad

- **Confidencialidad** (privacidad)
- **Autenticación** (quién creó/envió datos)
- **Integridad** (no han sido alterados)
- **No-repudio** (la orden es firme)
- **Control de acceso** (previene uso indebido de recursos)
- **Disponibilidad** (permanencia, no-borrado)

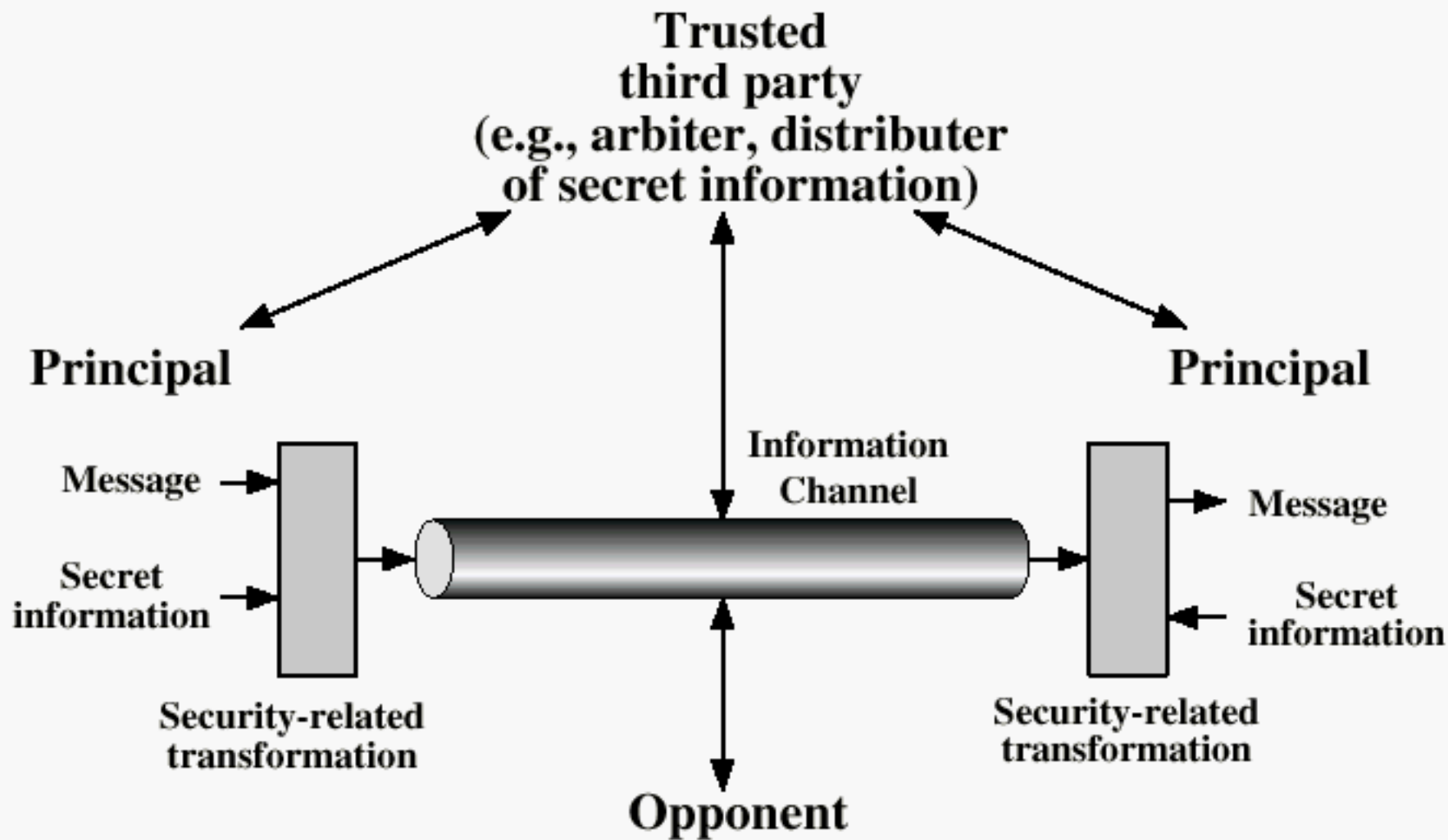
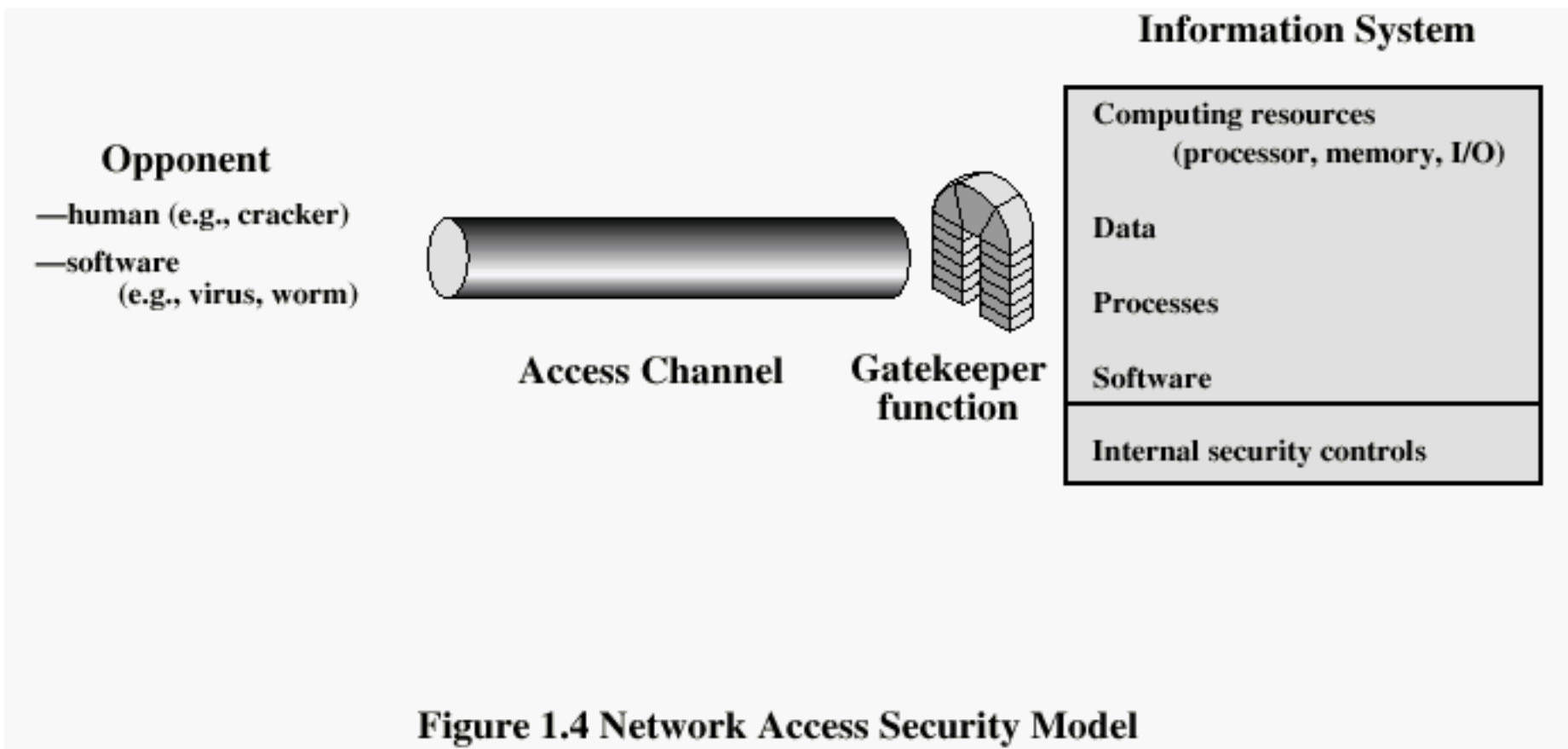


Figure 1.3 Model for Network Security



Métodos de Defensa

- Cifrado
- Controles por software (límites para acceso a BD; protección entre usuarios por el S.O.)
- Controles por hardware (*smartcard*)
- Políticas (cambio de claves)
- Controles físicos

Estándares

- En Internet: RFC (Solicitud de Comentarios)
 - Algoritmos, tecnologías
- Seguridad de la Información: serie ISO 27000
- Gestión de Servicios TI
 - ITIL
 - COBIT