Sistemas distribuidos de detección de intrusos

Antonio Villalón Huerta

toni@aiind.upv.es

Abril, 2004

This is 100% Microsoft free

Contenidos

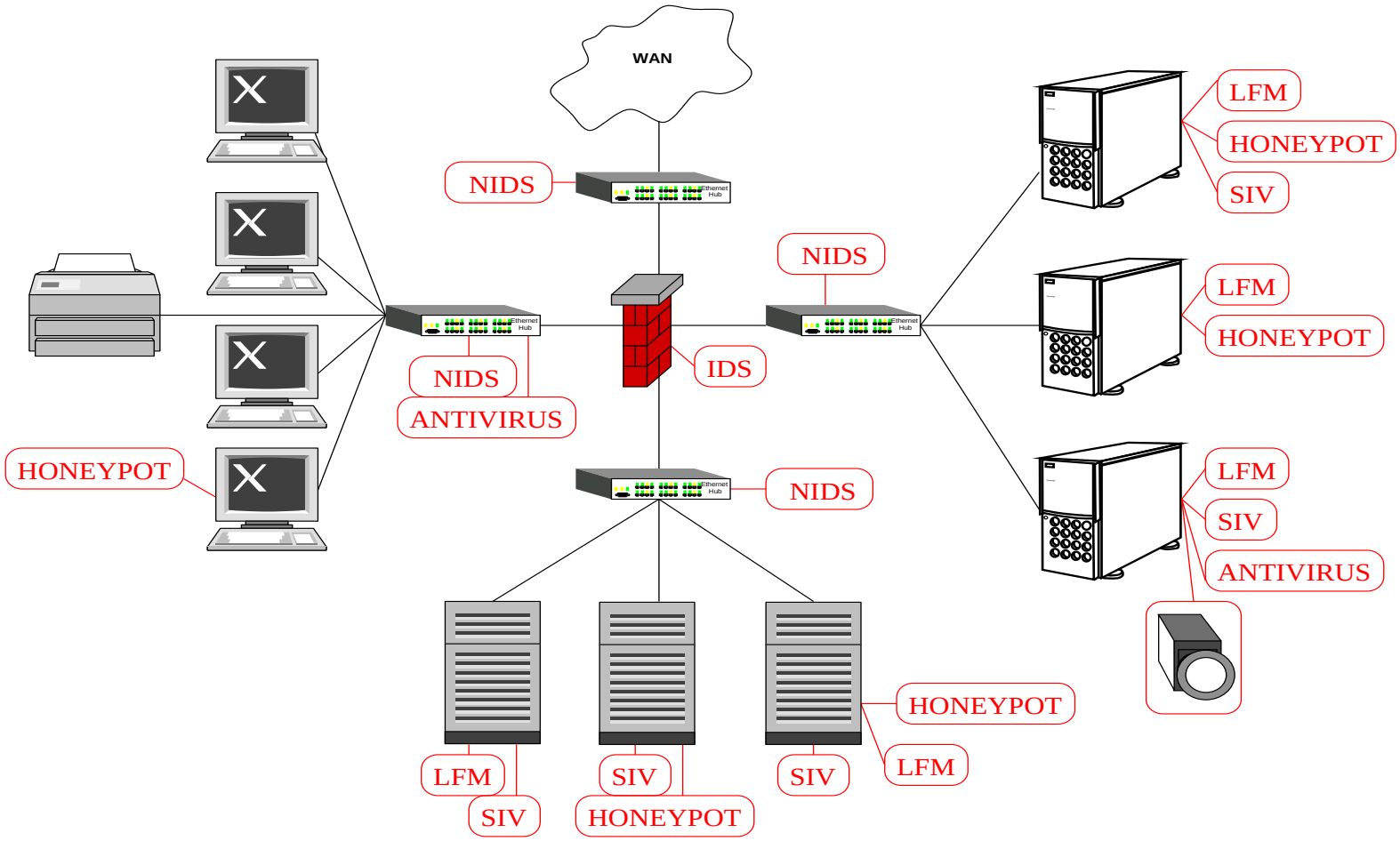
- Introducción.
- DIDS.
- Arquitectura.
- Problemas del esquema:
  - Comunicación.
  - Capacidad.
  - Inteligencia.
- Paquetes *software*.
- Líneas de trabajo.
- Conclusiones.

Introducción

Algunas definiciones

- **Intrusión:** Conjunto de acciones que intentan comprometer la integridad, confidencialidad o disponibilidad de un recurso.
- **Detección de intrusos:** Análisis automático de parámetros que modelan la actividad de un entorno con el propósito de detectar e identificar intrusiones.
- **Sistema de detección de intrusos (IDS):** Mecanismo de seguridad que lleva a cabo la detección de intrusos.
- **Sistema distribuido:** Conjunto de elementos autónomos enlazados entre sí mediante una red, que aparecen frente al usuario como un único sistema.
- **Evento:** Ocurrencia de un conjunto determinado de circunstancias.

El enfoque clásico



Problemas del enfoque

- Visión 'local': dificultad para detectar ciertos ataques.
- Gestión compleja ⇒ DESUSO.
- Escasa tolerancia a fallos.
- Escalabilidad nula.
- Costes de mantenimiento y operación elevados.
- **Muchos datos, poca información.**
- ...

DIDS

Una posible solución: DIDS

Llamamos sistema distribuido de detección de intrusos (DIDS) a aquel sistema de detección capaz de agregar eventos generados por diferentes fuentes, proporcionando así una imagen más amplia y detallada de las actividades maliciosas en un determinado entorno.

- *. . . diferentes fuentes. . .*
- *. . . capaz de agregar eventos. . .*
- *. . . imagen más amplia y detallada. . .*

DIDS

Algunas ideas...

- Entorno con múltiples IDSes potencialmente diferentes entre sí.
- Elementos que reciben información (eventos) de estos subsistemas...
- ...y aportan inteligencia adicional.
- Comunicación entre componentes del esquema.
- Humano que ve 'resumen' del estado en cada momento...y toma decisiones en función del mismo.
- Generalización del entorno: visión global de la seguridad.

Arquitectura

Componentes habituales de un DIDS

- 3+1 elementos básicos en un DIDS:
  - Agentes (monitorizan actividad).
  - Transceptores (comunicación).
  - Maestro/s (centralizan datos).
  - Consola de eventos (interfaz con operador).
- En entornos extremadamente sencillos $\nexists$ transceptores: comunicación unidireccional ('transmisores').
- Pueden definirse más componentes: generadores, *proxies*, actores, *clusters*...
- Nomenclatura confusa.

Arquitectura

Agente

- Entidad independiente que monitoriza algún tipo de actividad 'interesante'.
- Ejecutado de forma contínua o bajo demanda.
- No se comunica con otros agentes.
- Diferentes propósitos y lenguajes.
- De 0 a N en cada máquina.
- Nivel más bajo de la jerarquía.

Arquitectura

Transceiver

- 'Transceptor': transmisor + receptor.
- Un transceptor por cada máquina donde existe algún agente.
- Interfaz de comunicación entre agentes y maestros.
- Transmite información a un maestro (o a varios).
- Recibe órdenes de los maestros.

Arquitectura

Maestro

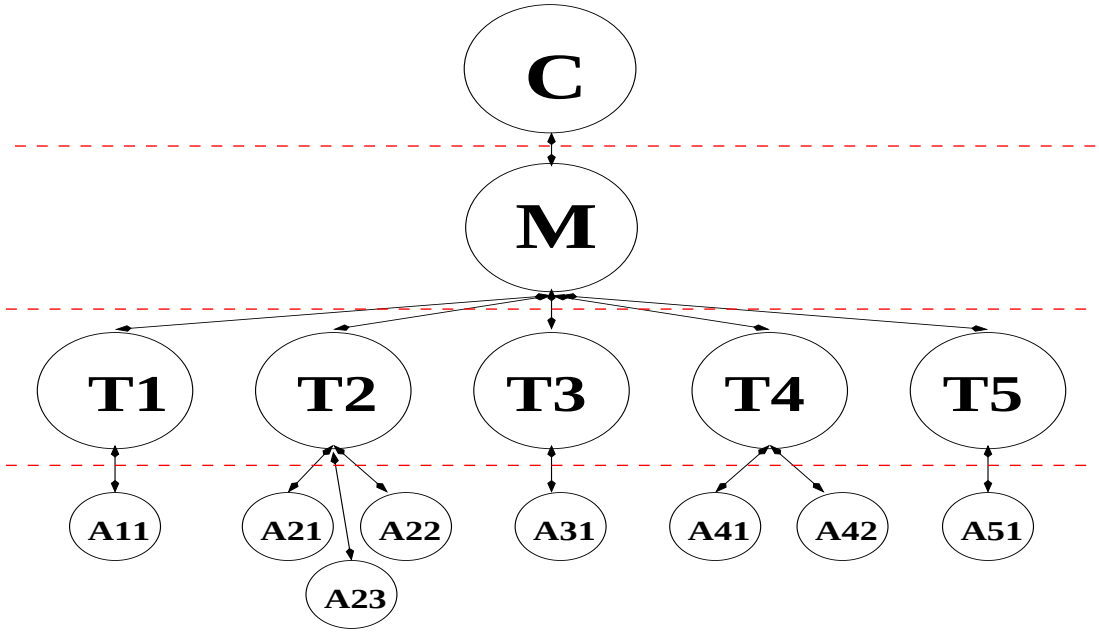
- Cerebro del esquema: alta importancia y complejidad.
- Recibe eventos de los transceptores (o de los agentes, en entornos simples).
- Detecta ataques incluso no notificados por transceptores.
- Control de agentes (y transceptores).
- Centralización de la información.
- Nivel máximo de inteligencia 'automática'.

Consola de eventos

- Elemento superior de la jerarquía.
- Interfaz del DIDS con un humano.
- Ayuda en la toma de decisiones.
- Quizás no es parte técnica del esquema pero...
- ...¿se podría eliminar del mismo?

Arquitectura

Un ejemplo gráfico...



- Un maestro (podríamos ampliar el esquema).
- Cinco subsistemas (cinco transceptores).
- N agentes en cada subsistema.
- Estructura **jerárquica** (lo habitual, aunque existen propuestas basadas en modelos no jerárquicos).

Problemas: comunicación

PROBLEMA: Todos los elementos del esquema deben 'hablar' un lenguaje común.

- Definición de estándares para el tratamiento de los datos de todos los elementos:
  - Vocabulario común.
  - Formato de la información.
  - Intercambio de datos entre elementos.
  - ...
- Dos ejemplos de formalización: CIDF e IDEF.
- SUBPROBLEMA: Fabricantes de sistemas de detección.

Problemas: comunicación

CIDF (*Common Intrusion Detection Framework*)

- Promovido por DARPA (*Defense Advanced Research Projects Agency*).
- Orientado a proyectos de investigación en detección de intrusos.
- Escasa aceptación comercial.
- Define:
  - Protocolos de comunicación entre elementos.
  - Lenguaje para la representación de datos de ID: CISL (*Common Intrusion Specification Language*).
- Proyecto finalizado en 1999.
- Más información: `http://gost.isi.edu/cidf/`

Problemas: comunicación

IDEF (*Intrusion Detection Exchange Format*)

- Definido por el *Intrusion Detection Working Group*, de IETF.
- Orientación comercial: IDWG está formado por empresas relacionadas con la detección de intrusos, en desacuerdo con parte del trabajo de CIDF.
- Define:
  - Protocolos de comunicación: *Intrusion Detection Exchange Protocol* (IDXP).
  - Modelo de datos: *Intrusion Detection Message Exchange Format* (IDMEF).
- Más información:
  `http://www.ietf.org/html.charters/idwg-charter.html`

Problemas: capacidad

PROBLEMA: Gran cantidad de información a procesar.

- Incremento de los requerimientos *hardware* (tanto a nivel de máquina como de red) y *software*.
- Optimización de algoritmos de procesamiento (maestro/s).
- Replicación de la jerarquía: elementos intermedios que aportan inteligencia (y reducen los datos intercambiados).
- Aumento de la inteligencia de los agentes: extracción y transmisión de los datos más significativos.

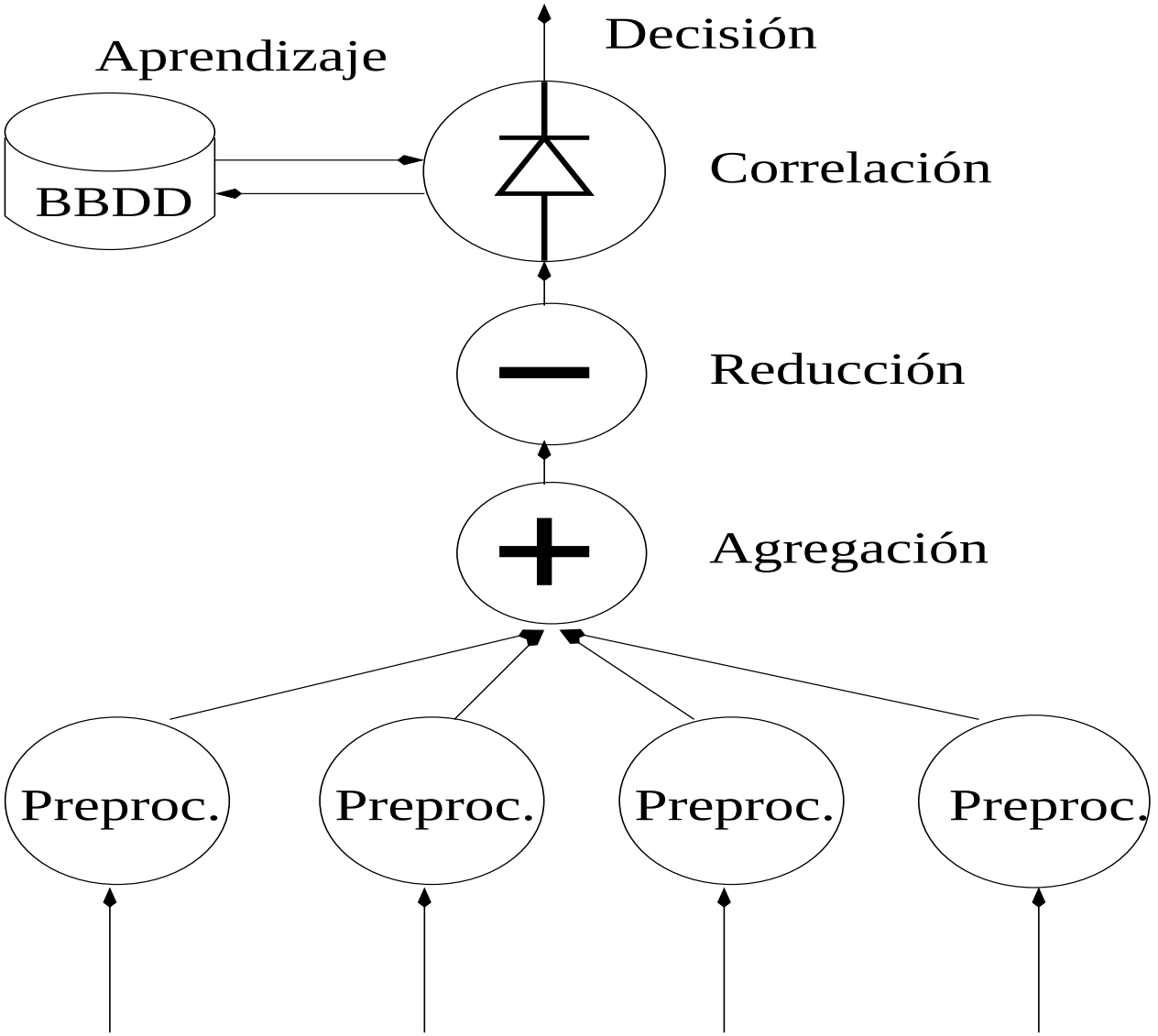
Problemas: inteligencia

PROBLEMA: ¿Cómo tratar los datos para generar 'inteligencia'?

- Preproceso: normalización y control de errores de los datos recibidos de los agentes.
- Agregación: agrupación y ordenación de alertas.
  $\Rightarrow$ Sincronización de relojes en cada elemento.
- Reducción: detección de alertas duplicadas.
  $\Rightarrow$ Proyecto: CIEL (*Common Intrusion Event List*).
- Correlación: detección de las relaciones entre eventos.
- Aprendizaje: realimentación del maestro para determinar nuevas relaciones y estados.
- Decisión: alerta a un operador, respuesta automática...

Problemas: inteligencia

Gráficamente...



Paquetes software

Algunos productos del mercado:

- IBM Tivoli Risk Manager
- NetForensics Security Information Management
- ArcSight Enterprise Security Management
- Tenable Network Security Lightning Console
- Prelude (*Open Source*)

Problemas habituales:

- Gestión compleja.
- Integración con productos de terceros.
- Correlación.
- €, \$, £, ¥...

Líneas de trabajo

To do...

- Correlación de eventos.
- Detección multipunto.
- Detección de ataques no conocidos.
- Sistemas tolerantes a fallos.
- Interfaces de comunicación.
- Respuesta automática.
- Gestión simplificada.
- ...

Conclusiones

- Necesidad de los sistemas de detección distribuidos.
- Beneficios de los estándares. ¿Integración de los fabricantes?
- Muchos problemas técnicos aún por resolver: campo activo de la investigación en seguridad informática.
- Principal problema no técnico: €.
- Futuro: ¿HIDS? ¿NIDS? ¿*honeypots*?. . . seguramente, **DIDS**.

¡¡Muchas gracias a todos!!