

Sistemas de Detección de Intrusos

Índice de materias

- Introducción.
- Clasificación de los IDSes.
- Implementación.
- Ejemplos de IDSes.
- Respuesta automática.
- Conclusiones.
- Referencias.

Introducción: definiciones

- Intrusión: Conjunto de acciones que intentan comprometer la integridad, confidencialidad o disponibilidad de un recurso.
 - No sólo penetraciones contra un sistema.
- Sistema de detección de intrusos: mecanismo cuyo objetivo es detectar, identificar y responder ante una intrusión.
 - No tiene por qué ser un programa o producto concreto.
- ¿Por qué un IDS?

Introducción: historia

- Primer trabajo sobre IDSes: 1980 (James P. Anderson).
- Década de los 80: diseño del primer sistema (IDES), que funcionaba en tiempo real (Dorothy Denning, Peter Neumann).
- Auge desde 1995 (crisis de los *firewalls*).
- Actualmente, uno de los campos con más investigación y avances.

Clasificación de los IDSes

- En función del origen de los datos a analizar:
 - IDSes basados en máquina (HIDS, *Host-based IDS*).
 - IDSes basados en red (NIDS, *Network-based IDS*).
- En función de la técnica de análisis utilizada:
 - Detección de anomalías (*Anomaly detection*).
 - Detección de usos indebidos (*Misuse detection*).
- Otras clasificaciones:
 - Tiempo real vs. periódicos.
 - Activos vs. pasivos.
 - Centralizados vs. distribuidos.
 - ...

Clasificación → Origen de datos → HIDS

- Sólo procesa datos asociados a un recurso.
- Tipos:
 - Verificadores de integridad del sistema (SIV, *System Integrity Verifiers*).
 - Monitores de registros (LFM, *Log File Monitors*).
 - Sistemas de decepción (*Deception Systems*).

Clasificación → Origen de datos → NIDS

- Procesa datos asociados a varios recursos.
- No tienen por qué estar ubicados en **toda** la red (de hecho casi ningún NIDS lo está).
- En la actualidad, los más utilizados.

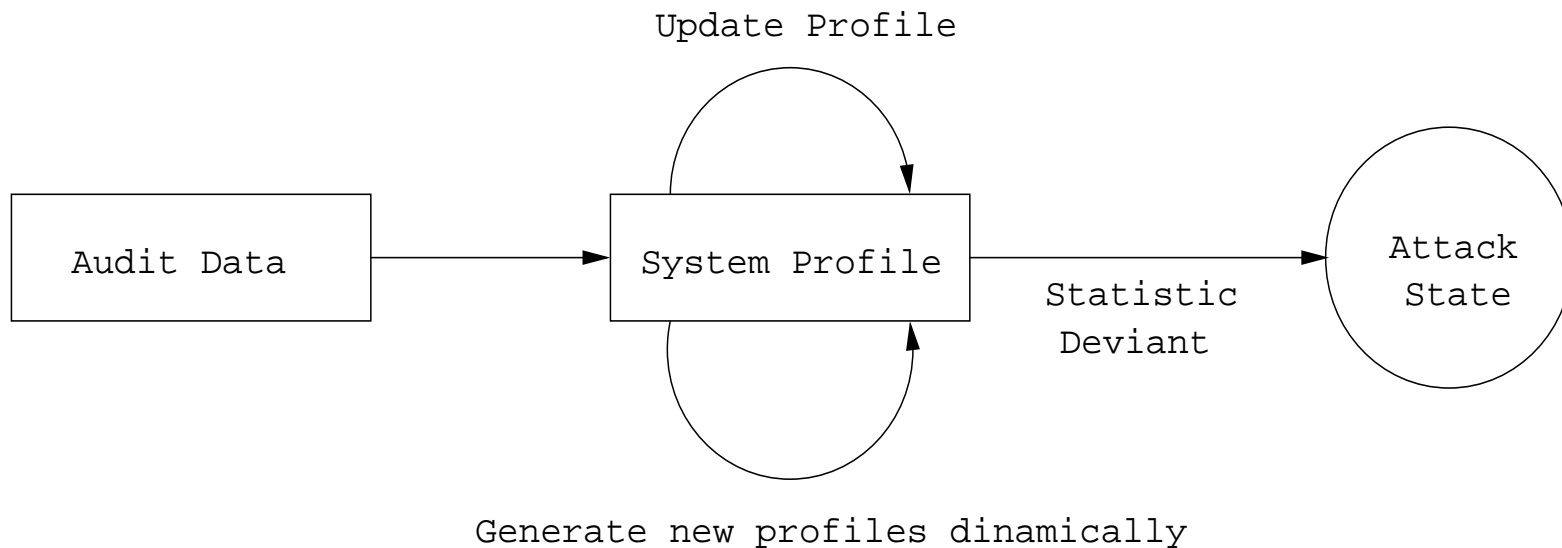
Sistemas de Detección de Intrusos

Clasificación → **Técnica de análisis** → *Anomaly Detection*

- IDEA: Una intrusión es una anomalía. Conozco lo que es ‘normal’ en un sistema, para poder detectar lo que no lo es (anomalías).
- PROBLEMA: La modelización del comportamiento es **muy compleja**.
- Sistemas expertos o aprendizaje automático (redes neuronales, reconocimiento geométrico...).
- Poco utilizados en sistemas reales.

Sistemas de Detección de Intrusos

Clasificación → **Técnica de análisis** → *Anomaly Detection*



[*An introduction to intrusion detection.* Aurobindo Sundaram, ACM Crossroads Student Magazine, 1996]

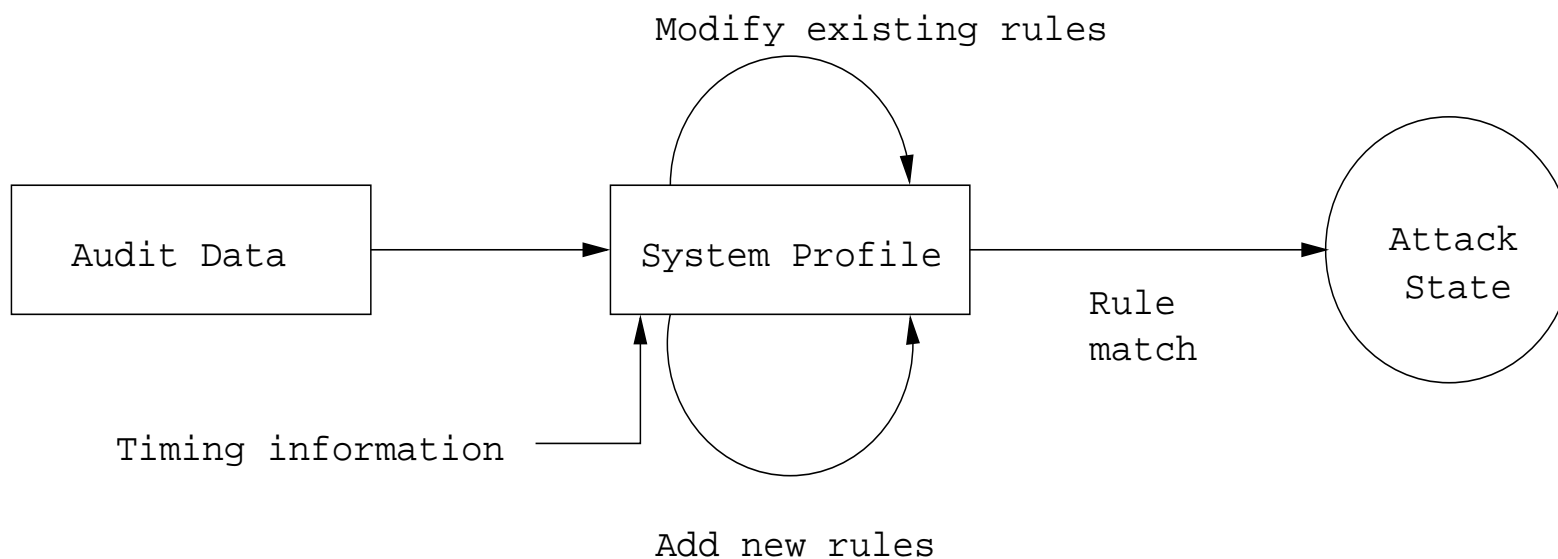
Sistemas de Detección de Intrusos

Clasificación → **Técnica de análisis** → *Misuse Detection*

- IDEA: No conozco lo que es ‘normal’ en un sistema, sino que directamente conozco lo anormal y lo puedo detectar.
- PROBLEMA: Sólo detecto los ataques que conozco.
- Diferentes aproximaciones. La más habitual: sistemas expertos.
- *Pattern Matching*: cada intrusión tiene un patrón asociado.
- En la actualidad, los más utilizados en sistemas reales.

Sistemas de Detección de Intrusos

Clasificación → **Técnica de análisis** → *Misuse Detection*



[*An introduction to intrusion detection.* Aurobindo Sundaram, ACM Crossroads Student Magazine, 1996]

Clasificación → Otros

- Tiempo real vs. Periódicos:

La monitorización del IDS es permanente.

IDSes pasivos \equiv analizadores de vulnerabilidades. ¿Se pueden considerar realmente IDSes?

- Activos vs. Pasivos:

El IDS es capaz de iniciar una respuesta automática.

- Centralizados vs. Distribuidos:

El IDS y la lógica asociada al mismo se implementan en un único sistema.

Implementación: IDS en el cortafuegos

- ¿Qué información maneja mejor un cortafuegos?
- Ataques más fáciles de detectar:
 - Escaneos de puertos.
 - Ciertos troyanos.
 - Patrones de tráfico sospechoso (por ejemplo, campos de la cabecera IP con un determinado valor).

Implementación: IDS en la red

- ¿Por qué?
- Cuestiones de diseño:
 - Número de sensores.
 - Ubicación de los sensores: ¿qué hacer en una arquitectura basada en *switches*?

Implementación: IDS en el *host*

- ¿Por qué?
- Análisis de *logs*.
- Verificadores de integridad.
- Problemas del esquema: ¿qué sucede si un pirata controla totalmente la máquina?

Implementación: Sistemas de decepción

- ¿Por qué ‘decepcionar’? *Negative knowledge*.
- Peligros de la decepción.
- Ejemplos simples de sistemas de decepción.

Implementación: DIDS

- Problema genérico de nuestro esquema: ¿Cómo integrar elementos?
- Sistemas distribuidos de detección de intrusos.
- Centralización: *master/slaves*.
- Comunicación entre elementos: CIDF, IDMEF, IDXP...
- Correlación de ataques: respuesta única, estadísticas, *forensics*...

Ejemplos de IDSes: SNORT

- <http://www.snort.org/>
- NIDS, *misuse detection* (sistema experto), tiempo real...
- Sistema abierto: muchas herramientas de terceros.
- ¡Gratuito!

Ejemplos de IDSes: *RealSecure*

- Internet Security Systems, Inc. (<http://www.iss.net/>).
- NIDS, *misuse detection* (sistema experto), tiempo real...

Ejemplos de IDSes: *Tripwire*

- Tripwire, Inc. (<http://www.tripwire.com/>).
- HIDS (verificador de integridad).

Respuesta automática

- Ventajas de un esquema de AR.
- Tipos de respuesta automática: defensa, ataque, recuperación y decepción.
- Precauciones **obligatorias** en un esquema de AR:
 - Ponderación de ataques (probabilidad ser falso positivo).
 - Direcciones protegidas.
 - Número de respuestas por unidad de tiempo.

Conclusiones

- Importancia de la detección.
- Sistemas actuales: débiles (no detección de ataques nuevos) pero necesarios.
- IDS como mecanismo, no como producto concreto: DIDS.
- El futuro:
 - Sistemas distribuidos.
 - Detección de nuevos tipos de ataques (*novel attacks*).
 - Refinamiento de la respuesta automática.

Sistemas de Detección de Intrusos

Algunas referencias...

- Intrusion Detection: Network Security beyond the Firewall. Terry Escamilla. John Wiley & Sons, 1998.
- Network Intrusion Detection: An Analyst's Handbook. Stephen Northcutt, Donald McLachlan, Judy Novak. New Riders Publishing, 2000 (2nd Edition).
- Intrusion Detection: Generics and State of the Art. NATO Research & Technology Organisation. Technical Report RTO-TR-049. NATO, 2002.
- COAST IDS pages:
<http://www.cerias.purdue.edu/coast/intrusion-detection/welcome.html>
- Intrusion Detection Working Group:
<http://www.ietf.org/html.charters/idwg-charter.html>