PUCE Virtual

DOCUMENTO DE PROFUNDIZACIÓN

Programación III

Implementación de Árboles AVL para Monitoreo en Tiempo Real en un Centro de Operaciones de Seguridad (SOC)

Estudio de caso 2: Implementación de Árboles AVL para Monitoreo en Tiempo Real en un Centro de Operaciones de Seguridad (SOC)

Contexto

Una empresa de telecomunicaciones gestiona más de 5 millones de eventos diarios generados por firewalls, sistemas IDS/IPS, routers y servidores críticos.

Los eventos deben analizarse en tiempo real para detectar:

- Ataques de fuerza bruta
- Escaneos de puertos
- Actividad sospechosa por IP
- Picos anómalos de tráfico

Inicialmente, se utilizó un Árbol Binario de Búsqueda (BST) para indexar eventos por dirección IP. Sin embargo, muchas IPs llegaban en orden creciente, lo que provocó desbalance en el árbol.

Problema

Debido al ingreso secuencial de datos:

- El BST se degeneró en una estructura similar a lista enlazada.
- El tiempo de búsqueda pasó de O(log n) a O(n).
- El sistema comenzó a presentar retrasos en la correlación de eventos.
- Se generaron cuellos de botella en momentos de alta carga.

En un escenario de ataque DDoS, cada segundo es crítico.

Solución Propuesta

Migrar la estructura de indexación a un **Árbol AVL**, que garantiza balance automático tras cada inserción.

Estrategia:

- Indexar eventos por IP o timestamp.
- Aplicar rotaciones automáticas cuando el factor de equilibrio supere ±1.
- Mantener altura mínima del árbol.

Implementación

1. Insertar evento.
2. Calcular altura del nodo.
3. Verificar factor de equilibrio.
4. Aplicar rotación simple o doble si es necesario.
5. Mantener estructura balanceada.

Resultados

Métrica	**BST Desbalanceado**	**AVL**
Tiempo de búsqueda promedio	4.5 s	0.8 s
Rendimiento en alta carga	Inestable	Estable
Complejidad garantizada	O(n)	O(log n)

Se logró una mejora del 82% en eficiencia de búsqueda.

Impacto en Ciberseguridad

- Detección más rápida de ataques masivos.
- Mayor estabilidad en análisis en tiempo real.
- Mejor escalabilidad ante crecimiento de logs.
- Reducción de consumo de CPU en procesos de consulta.

Reflexión Técnica

En sistemas de ciberseguridad donde los datos llegan continuamente y pueden seguir patrones ordenados (por IP o timestamp), el uso de un BST simple puede ser riesgoso.

El Árbol AVL ofrece una garantía formal de eficiencia en el peor caso, lo que lo convierte en una solución adecuada para:

- Sistemas SIEM
- Plataformas de monitoreo continuo

- Motores de correlación de eventos
- Análisis forense automatizado

En entornos críticos, la auto-regulación estructural del AVL no es solo una mejora algorítmica, sino una ventaja estratégica en la defensa digital.