



SEGURIDAD EN BASE DE DATOS

ARQUITECTURA DE SUBCONJUNTO TCB



RICARDO - ANGEL

INTRODUCCIÓN



La Arquitectura de Subconjunto del TCB es un concepto crucial en la seguridad informática. Esta arquitectura se enfoca en la parte crítica de un sistema informático que debe ser confiable para garantizar la seguridad y la integridad de la información.

¿QUE ES?



Es un enfoque de diseño de sistemas informáticos que se centra en identificar y minimizar los componentes críticos que forman parte de la Base de Confianza (TCB).

PRINCIPIOS

MINIMIZACIÓN

Reducir al mínimo el tamaño y la complejidad de la base de confianza de computación, manteniendo solo las funcionalidades críticas para la seguridad.

AISLAMIENTO

Las partes críticas deben estar estrictamente aisladas del resto del sistema para evitar posibles ataques.

VERIFICACIÓN Y VALIDACIÓN

Cada componente incluido en el subconjunto del TCB debe ser rigurosamente verificado y validado para garantizar su integridad y fiabilidad.

TRANSPARENCIA

Significa que las operaciones dentro del TCB deben ser comprensibles y auditables para garantizar la confianza en el sistema.

BENEFICIOS

MAYOR SEGURIDAD

Al minimizar la cantidad de código y funcionalidad en el TCB, se reduce la superficie de ataque potencial, lo que mejora la seguridad general del sistema.

FACILITA LA AUDITORÍA

Con un TCB más pequeño y transparente, la auditoría y la supervisión del sistema se vuelven más efectivas y manejables.

BENEFICIOS

MENOR COMPLEJIDAD

Al eliminar componentes no esenciales del TCB, se reduce la complejidad del sistema, lo que facilita el mantenimiento y la resolución de problemas.

MEJOR DESEMPEÑO

Con un TCB más pequeño y eficiente, el rendimiento del sistema puede mejorar, ya que hay menos carga en los componentes críticos.

CONCLUSIÓN



La Arquitectura de Subconjunto TCB es un enfoque fundamental en el diseño de sistemas de seguridad informática que busca maximizar la confiabilidad y la integridad al minimizar la superficie de ataque. Al identificar y aislar las partes esenciales del sistema, se puede mejorar significativamente la seguridad sin comprometer la funcionalidad o el rendimiento. Es un principio clave para construir sistemas informáticos más seguros y confiables en un mundo cada vez más conectado y digitalizado.