Resumen Libro y Pdfs

Libro

Capítulo 9: Replicación, Consistencia y Tolerancia a Fallas

Objetivo del Capítulo:
Analizar y comprender los esquemas de replicación, consistencia y tolerancia a fallas, y su impacto en el diseño de sistemas distribuidos.

Contenido Detallado:
1. Introducción:
- Se discute la importancia de la replicación para mejorar la confiabilidad y el rendimiento en sistemas distribuidos, así como los desafíos de mantener las réplicas consistentes.

2. Replicación:
- Se describen los beneficios de la replicación en términos de rendimiento, alta disponibilidad y tolerancia a fallas.
- Se presentan los requisitos para implementar replicación efectiva, incluyendo la transparencia y la consistencia.
- Se introduce el modelo general de gestión de réplica y su arquitectura básica, destacando el rol del gestor de réplicas y del frontend.

3. Servicios de Tolerancia a Fallas Basados en Replicación:
- Se diferencian los métodos de replicación pasiva y activa, detallando las fases de ejecución y cómo cada uno maneja las fallas.

Capítulo 10: Seguridad

Objetivo del Capítulo:
Proporcionar una visión general sobre la importancia de la seguridad en sistemas distribuidos, centrada en el cifrado y la autenticación de acceso.

Contenido Detallado:
1. Introducción:

- Se aborda la seguridad desde una perspectiva de procedimientos y medidas tanto lógicas como físicas para prevenir, detectar y corregir mal uso.

2. Ataques a la Seguridad:
- Se describen los tipos de ataques (interrupción, intercepción, modificación y fabricación) y cómo estos pueden afectar la seguridad de la información.

3. Servicios de Seguridad:
- Se exploran servicios esenciales como confidencialidad, autenticación, integridad, vinculación y control de acceso, y cómo estos servicios utilizan mecanismos de seguridad para proteger el sistema.

4. Mecanismos de Seguridad:
- Se discuten técnicas criptográficas clave para garantizar la seguridad, incluyendo el intercambio de autenticación, encriptado, integridad de datos, firma digital, y control de acceso.

Capítulo 11: Multimedia Distribuida

Objetivo del Capítulo:
Comprender los aspectos técnicos y de infraestructura del flujo de video y su importancia en los sistemas distribuidos.

Contenido Detallado:
1. Introducción:
- Se definen los medios multimedia y se destaca el video como el medio ideal por combinar texto, sonidos e imágenes.

2. Estándares de Codificación de Video:
- Se revisan los estándares de compresión de video como H.261, MPEG-1, H.262 (MPEG-2), y otros, resaltando su evolución y la importancia de cada uno en la reducción de la tasa de bits.

3. Distribución de Video:
- Se discuten las tecnologías y sistemas de distribución de video, incluyendo video bajo demanda y video IP, y los desafíos asociados con la calidad de servicio y la latencia.

El documento titulado "1. Seguridad"

Conceptos Generales
- Seguridad y Protección: Definidos como la medida de confianza en que se mantendrá la integridad de un sistema y sus datos. La protección se refiere a los mecanismos que controlan el acceso de procesos y usuarios a los recursos del sistema.

Amenazas y Ataques
- Amenazas y Ataques: Se discuten las diferencias entre una amenaza, que es una violación potencial, y un ataque, que es un intento de explotar esa vulnerabilidad. Los ataques pueden ser accidentales o maliciosos, y es más fácil protegerse contra usos accidentales que maliciosos.

Propiedades de la Seguridad
- Propiedades Clave: Incluyen la confidencialidad (prevención de la revelación de datos), la integridad (prevención de la corrupción de datos), y la disponibilidad (prevención de denegación de servicio).

Violaciones de Seguridad
- Categorías de Violaciones: Como fallas de confidencialidad, integridad, y disponibilidad, robo de servicio y negación de servicio.
- Métodos de Ataques: Incluyen la mascarada (brecha de autenticación), ataque replay, modificación de mensajes, hombre en el medio, y toma de control de sesión.

Niveles de Medidas de Seguridad
- Medidas Multinivel: La seguridad efectiva debe existir en múltiples niveles — físico, sistema operativo, red y aplicaciones.

Modelos de Seguridad
- Modelo de Cuatro Capas: Discussión sobre cómo proteger cada capa de la infraestructura tecnológica, desde el hardware físico hasta las aplicaciones.

Programas Peligrosos
- Tipos de Programas Maliciosos: Como caballos de Troya, puertas traseras, bombas lógicas, y rebosamientos de buffer.

Criptografía

- Uso de Criptografía: Detalla cómo la criptografía es esencial para la seguridad, describiendo la criptografía de clave secreta y pública, y cómo estas técnicas permiten la encriptación y desencriptación de mensajes.

Autenticación de Usuario
- Métodos de Autenticación: Incluye detalles sobre cómo las contraseñas y otros métodos autentican a los usuarios y protegen contra el acceso no autorizado.

Control de Acceso
- Matriz de Acceso: Explicación sobre cómo las matrices de acceso regulan qué procesos pueden acceder a qué recursos dentro de un sistema informático.

El documento titulado "2 herramientas de seguridad"

Introducción a la Seguridad
- Hipótesis Básicas: Se enfatiza la importancia de hacer hipótesis sobre posibles amenazas y validar las técnicas de seguridad mediante pruebas formales. Se destaca la necesidad de técnicas de auditoría debido a que ninguna lista de amenazas es exhaustiva.
- Amenazas a la Seguridad: Incluye la filtración, adulteración, robo de recursos y vandalismo.
- Métodos de Ataque: Se discuten métodos específicos como fisgoneo, mascarada, adulteración de mensajes y retransmisión diferida.

Criptografía
- Claves Simétricas y Asimétricas: Se explican los fundamentos de la criptografía, incluyendo la diferencia entre claves simétricas (donde la clave de encriptación y desencriptación son iguales) y asimétricas (donde difieren).
- Algoritmos y Técnicas: Se detalla el uso de diversos algoritmos como DES y RSA, explicando su funcionamiento y seguridad.

Firmas Digitales
- Fundamento y Implementación: Se describen las firmas digitales como garantía de autenticidad y no modificación de mensajes. También se explican los procesos de implementación utilizando funciones sintetizadoras como MD5 y SHA-1.

- Uso de Claves Públicas en Firmas: Se discute el proceso de autenticación utilizando firmas digitales con claves públicas, y el rol de las entidades certificadoras.

Autenticación y Distribución de Claves
- Problemática y Soluciones: Se expone cómo se autentifican y distribuyen claves en sistemas distribuidos, mencionando el protocolo de Needham-Schroeder y otros mecanismos basados en claves simétricas y públicas.
- Seguridad en la Distribución de Claves: Se abordan las técnicas para asegurar que las claves distribuidas no sean accesibles para atacantes y cómo se utiliza la criptografía para proteger estas claves.

Casos de Estudio
- Kerberos: Se profundiza en el funcionamiento de Kerberos, un protocolo para sistemas seguros de autenticación basado en tickets.
- SSL y Java 1.2: Se mencionan brevemente otros ejemplos de aplicaciones de los conceptos de seguridad discutidos, como SSL y características de seguridad en Java 1.2.

El documento titulado "Ejemplo políticas de seguridad"

Políticas de Seguridad Informática

1. Política de Uso Aceptable (AUP)
- Objetivo: Prevenir el uso indebido de recursos informáticos.
- Contenido: Directrices sobre el uso apropiado de internet, correo electrónico, software autorizado y dispositivos personales.

2. Política de Gestión de Contraseñas
- Objetivo: Asegurar que las contraseñas sean robustas y seguras.
- Contenido: Requisitos sobre la longitud, complejidad, y manejo seguro de contraseñas.

3. Política de Control de Acceso
- Objetivo: Garantizar accesos adecuados y seguros a los sistemas y datos.
- Contenido: Asignación de roles, uso de autenticación multifactor y revisión periódica de accesos.

4. Política de Respuesta a Incidentes
- Objetivo: Minimizar impactos de incidentes de seguridad y restaurar operaciones normales rápidamente.
- Contenido: Procesos para detectar, reportar y mitigar incidentes.

5. Política de Copias de Seguridad
- Objetivo: Asegurar la disponibilidad y recuperación de datos en caso de pérdida o corrupción.
- Contenido: Frecuencia de backups, almacenamiento seguro y procedimientos de restauración.

6. Política de Gestión de Parches
- Objetivo: Mantener los sistemas actualizados y protegidos contra vulnerabilidades.
- Contenido: Proceso de aplicación de parches y actualizaciones de software.

7. Política de Seguridad de Datos
- Objetivo: Proteger la integridad, confidencialidad y disponibilidad de los datos.
- Contenido: Clasificación de datos, métodos de cifrado y manejo seguro de la información.

8. Política de Seguridad Física
- Objetivo: Proteger los activos informáticos contra accesos físicos no autorizados y daños.
- Contenido: Control de accesos físicos y medidas contra desastres naturales y robos.

9. Política de Seguridad en Desarrollo de Software
- Objetivo: Asegurar que el software desarrollado esté libre de vulnerabilidades conocidas.
- Contenido: Revisión de código, pruebas de seguridad y control de versiones.

10. Política de Formación y Concienciación en Seguridad
- Objetivo: Incrementar la consciencia sobre las amenazas de seguridad y promover prácticas seguras.
- Contenido: Programas de formación, campañas de concienciación y evaluación del conocimiento.

11. Política de Gestión de Riesgos
- Objeto: Reducir la probabilidad e impacto de incidentes de seguridad.
- Contenido: Análisis y mitigación de riesgos de seguridad.

12. Política de Uso de Dispositivos Móviles
- Objetivo: Proteger la información en dispositivos móviles y reducir riesgos asociados.
- Contenido: Seguridad para dispositivos, cifrado de datos y políticas de acceso remoto.

Además, se incluyen normativas específicas de Chile relacionadas con la protección de datos personales y la regulación de la ciberseguridad, como la Ley N° 19.628 sobre Protección de la Vida Privada y la Ley N° 21.096 que crea la Agencia Nacional de Ciberseguridad.

El documento titulado "Seguridad en ambientes Distribuidos"

Introducción
- Presentación: A cargo de Jorge Rojas Zordan, experto en seguridad informática, quien aborda la evolución de las amenazas de seguridad y la importancia de sistemas de control adecuados en entornos distribuidos.

Evolución de las Amenazas de Seguridad
- Historia: Se describe el avance tecnológico desde la era de las punto com hasta la proliferación de redes sociales y dispositivos móviles, enfatizando cómo cada etapa ha planteado nuevos riesgos.
- Amenazas destacadas en 2011: Incluyen contraseñas débiles, transmisión de datos sensibles sin encriptación, y vulnerabilidades en servidores y dispositivos.

Conceptos Fundamentales de la Seguridad de la Información
- Impactos de los incidentes de seguridad: Se discuten los daños a la confidencialidad, integridad y disponibilidad de los datos.
- Modelos de seguridad: Se explica la implementación de controles de seguridad en un modelo de capas, desde periféricos hasta controles internos, para proteger eficazmente los activos de información.

Administración del Riesgo

- Proceso continuo: Se enfatiza en la gestión del riesgo como un proceso que incluye evaluación de amenazas, diseño de arquitecturas de seguridad, y establecimiento de un plan estratégico.

- Fuentes de riesgo: Se categorizan como naturales, ambientales y humanas.

Estrategias para Manejo de Riesgos

- Estrategias de mitigación: Se discuten métodos para reducir riesgos, incluyendo la implementación de controles específicos y la transferencia de riesgo a terceros.

- Balance entre impacto y inversión: Se debate cómo optimizar recursos en seguridad para mitigar los riesgos más significativos sin sobrecargar financieramente a la organización.

Tendencias y Desafíos Futuros

- Desafíos futuros: Se anticipan retos como la administración de dispositivos personales, la unificación de tecnologías y controles, y la mejora de las políticas de seguridad.

- Soluciones propuestas: Incluyen estrategias de autenticación integrada, controles dinámicos según las necesidades del negocio y medidas de seguridad adaptadas a la evolución tecnológica.

Conclusiones

- Adaptación de controles de seguridad: Se concluye que las organizaciones deben adaptar sus estrategias de seguridad a las cambiantes necesidades del negocio y mantener una gestión de seguridad proactiva y dinámica.