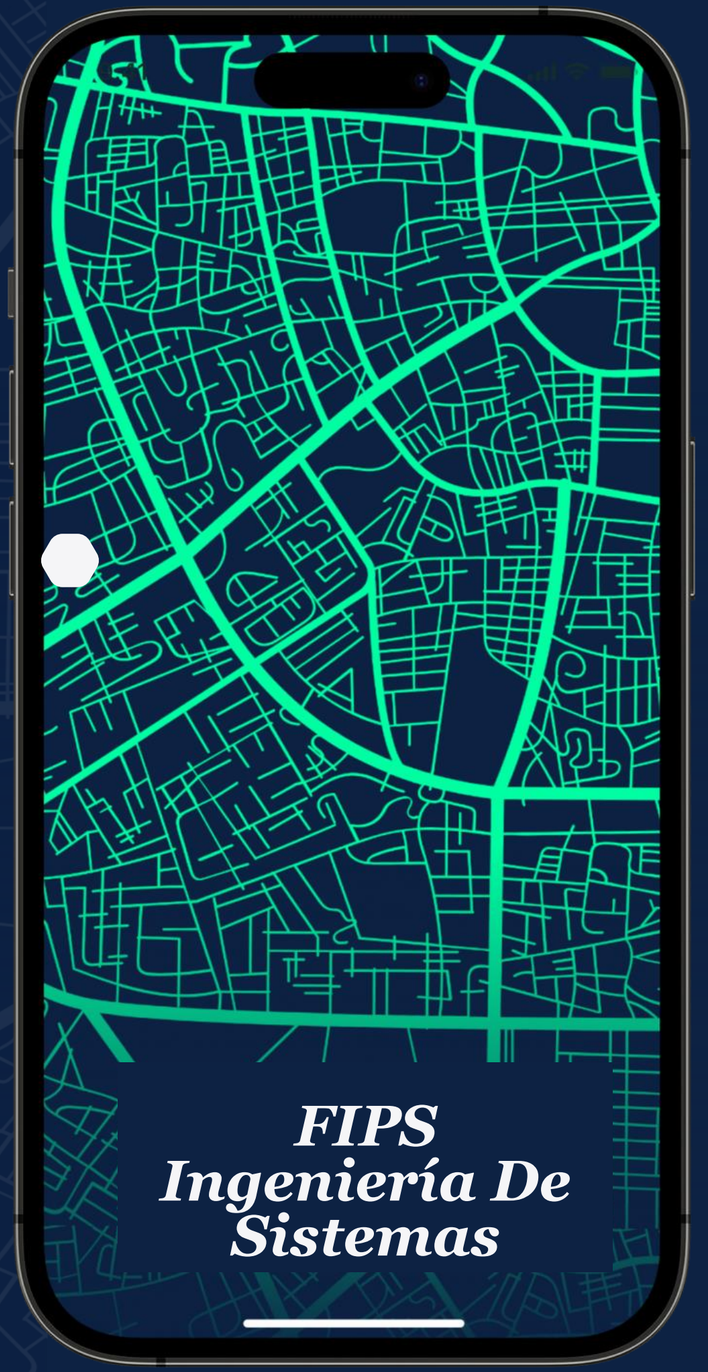
UNSA
UNIVERSIDAD NACIONAL DE SAN AGUSTIN DE AREQUIPA

Periodo Académico: 2025
Semestre: 07

SISTEMAS DISTRIBUIDOS



Capítulo IX: SEGURIDAD

Tema 14: Introducción, criptografía, autenticación, confianza en los sistemas distribuidos, autorización, monitoreo y ejemplos.

Docente. Mg. Maribel Molina Barriga

Contenido

Introducción a la Seguridad en Sistemas Distribuidos

- Un sistema distribuido es un conjunto de computadoras independientes que se presentan ante los usuarios como un sistema único.
- En los sistemas distribuidos, la seguridad de la información juega un rol muy importante, ya que se debe de garantizar que los recursos de cómputo y la información estén protegidos. Para un enfoque de seguridad informática se recomienda observar los siguientes aspectos:
- Objetivos de la seguridad:
  - Confidencialidad
  - Integridad
  - Disponibilidad
  - Autenticación
- La seguridad es crítica por la comunicación a través de redes inseguras.
- Amenazas comunes: interceptación, modificación, suplantación, denegación de servicio.

Criptografía

Criptografía en Sistemas Distribuidos

- Objetivo: proteger la confidencialidad e integridad de los datos.

- Tipos:
  - Simétrica (AES): Requiere compartir la clave para cifrar y descifrar. Rápida pero con problemas de distribución de claves
  - Asimétrica (RSA, ECC): clave pública y privada. Usada en HTTPS, VPNs, etc.

- Funciones hash: para verificación de integridad. Uso en comunicaciones seguras, almacenamiento distribuido, blockchain.

- Ejemplo: TLS/SSL para comunicaciones seguras.

- Herramientas: OpenSSL, GnuPG, NaCl (Networking and Cryptography library)

5

Autenticación

- Proceso para verificar identidad de usuarios y sistemas.
- Métodos:
  - Contraseña
  - Certificados digitales (X.509) (es un formato estandarizado para codificar e intercambiar certificados de clave pública)
  - Tokens (JWT, OAuth2)
  - Biometría

- En sistemas distribuidos: uso de Kerberos, LDAP (protocolo Ligero de Acceso a Directorios), y OAuth 2.0 para SSO (Single Sign-On).

JSON Web Token (abreviado **JWT**) es un estándar abierto basado en JSON propuesto por IETF (RFC 7519) para la creación de tokens de acceso que permiten la propagación de identidad y privilegios o *claims* en inglés. Por ejemplo, un servidor podría generar un token indicando que el usuario tiene privilegios de administrador y proporcionarlo a un cliente.

OAuth 2.0 es un protocolo de autorización abierto que permite a las aplicaciones acceder a recursos protegidos en nombre de un usuario, sin necesidad de compartir las credenciales de inicio de sesión del usuario.

El inicio de sesión único (SSO) es un método de autenticación que permite a los usuarios iniciar sesión en múltiples aplicaciones o sitios web con un único conjunto de credenciales, eliminando la necesidad de recordar y administrar nombres de usuario y contraseñas separados para cada servicio.

La biometría, en el ámbito de la seguridad informática, se refiere al uso de características físicas o de comportamiento únicas de una persona para verificar su identidad

Confianza en Sistemas Distribuidos

- La confianza no puede presuponerse: los nodos pueden estar comprometidos.
- Modelos de confianza:
  - Modelo de red confiable (limitado)
  - Modelo de confianza cero (Zero Trust Architecture)

- Se basa en políticas, certificados y comportamiento histórico.

https://learn.microsoft.com/en-us/security/zero-trust/zero-trust-overview

Autorización y Control de Acceso

- Define quién puede hacer qué después de autenticarse.
- Técnicas:
  - Listas de control de acceso (ACL)
  - RBAC (Control de Acceso Basado en Roles)
  - ABAC (Control Basado en Atributos)

- Herramientas: Keycloak, Open Policy Agent (OPA)

Monitoreo y Detección de Intrusos

- Importante para detectar actividades anómalas o maliciosas.
- IDS (Sistemas de detección de intrusos) y SIEM (Gestión de eventos e información de seguridad).
- Ejemplos:
  - Snort
  - OSSEC
  - Splunk
  - Wazuh

Técnicas de seguridad

Técnicas Actuales de Seguridad

- Zero Trust: no se confía en nada por defecto.
- Blockchain: para integridad y confianza descentralizada.
- Autenticación multifactor (MFA)
- Cifrado homomórfico: permite cálculos sobre datos cifrados.
- Seguridad basada en IA: para detectar patrones sospechosos

Herramientas de seguridad

Herramientas de Software de Seguridad

- Wireshark – Análisis de tráfico.
- Metasploit – Pruebas de penetración.
- Keycloak – Autenticación y autorización.
- Vault (HashiCorp) – Gestión de secretos.
- Wazuh – Monitoreo e IDS - (Sistema de Detección de Intrusiones)

Casos Reales de Seguridad en Sistemas Distribuidos

Caso 1: SolarWinds (2020)

- Ataque a la cadena de suministro de software.
- Comprometió múltiples agencias gubernamentales y empresas.
- https://www.e-dea.co/ataque-solarwinds-orion

Caso 2: Microsoft Exchange Server (2021)

Fallos de seguridad permitieron ejecución remota de código.
https://en.wikipedia.org/wiki/2021_Microsoft_Exchange_Server_data_breach

Caso 3: Cloudflare y Zero Trust (2022)

Implementación real de arquitectura Zero Trust para proteger su infraestructura global.
https://uvadoc.uva.es/bitstream/handle/10324/63026/TFG-G6508.pdf?sequence=1
https://www.cloudflare.com/es-es/zero-trust/products/access/

Actividad

Lee cuidadosamente las siguientes fuentes seleccionadas:
Modelo de Confianza Cero según NIST (https://csrc.nist.gov/pubs/sp/800/207/final)
Keycloak: Gestión de identidad y acceso (https://www.keycloak.org/)
Ataque SolarWinds – Análisis del caso (https://www.e-dea.co/ataque-solarwinds-orion)

Responde en un documento las siguientes preguntas de análisis:

- ¿Qué desafíos de seguridad enfrentan los sistemas distribuidos que no son tan frecuentes en sistemas centralizados?
- Explica brevemente la diferencia entre autenticación y autorización con ejemplos en sistemas distribuidos.
- ¿Qué es el modelo de Confianza Cero y por qué es relevante hoy en día para empresas con infraestructura distribuida?
- ¿Cómo contribuye herramienta como Keycloak a mejorar la seguridad de una organización?

Casos Reales
Resume el ataque SolarWinds: ¿qué falló y qué aprendizajes deja para la protección de entornos distribuidos?

Opinión personal
Desde tu punto de vista, ¿qué técnica o herramienta debería ser prioritaria para implementar en una universidad con servicios distribuidos (plataformas, sistemas académicos, correo, etc.)?
***Justifica tu respuesta*.**

Referencias

- G. Colouris, J. Dollimore,T. Kindberg and G. Blair. Distributed Systems: Concepts and Design (5th Ed). Addison-Wesley, 2011.
- A.S.Tanenbaum and M.V. Steen, Distributed Systems: Principles and Paradigms, Prentice Hall, 2006.
- https://csrc.nist.gov/pubs/sp/800/207/final
- https://owasp.org/
- https://www.wireshark.org/
- https://www.keycloak.org/
- https://owasp.org/
- https://www.splunk.com/
- https://www.snort.org/
- https://learn.microsoft.com/en-us/security/zero-trust/zero-trust-overview

GRACIAS.

mmolinab@unsa.edu.pe