Seguridad en los Sistemas Distribuidos

Jose Luis Molina Aguilar Jose Luis Rico Ramos David Martinez Diaz
Miguel Tirado Guzman Manuel Zafra Mota

18 de marzo de 2023

Índice

1. Lista de roles

- Jose Luis Molina Aguilar - Crítico
- Jose Luis Rico Ramos - Proponente
- David Martinez Diaz - Preguntador
- Miguel Tirado Guzman - Resumidor
- Manuel Zafra Mota - Proporcionador de Ejemplos

2. Resumen

La seguridad es un aspecto clave en los Sistemas Distribuidos, siendo muy importante en la actualidad debido al crecimiento exponencial en número ciberataques que ha ido surgiendo en los últimos años. Es por esto por lo que hemos decidido realizar un proyecto tratando este tema.

En este abordaremos en un inicio una introducción al problema de la seguridad (además de la definición de sistema distribuido) y el por qué es un aspecto tan importante. A continuación daremos una descripción de qué se entiende por seguridad en un sistema distribuido y , por tanto, sabremos cuándo podemos decir que es seguro un sistema distribuido y las comunicaciones entre sus componenes.

Acto seguido pasamos a definir e identificar los mecanismos básicos sobre los que se implementa la seguridad en los sistemas distribuidos además de la definición de otros procedimientos no tan básicos que también ayudan a prevenir ataques. Decidimos que lo mejor era centrarnos en explicar las técnicas básicas porque las más avanazdas siempre se basan en ellas. (Tanto el cifrado de una comunicación como de una base de datos se van a basar en la criptografía). Una vez identificados dichos mecanismos daremos una serie de desventajas que también conllevan.

Por último damos una serie de conclusiones discutiendo sobre la superación o no superación de las distintas desventajas que plantean los mecanismos vistos anteriormente.

3. Introducción

La **seguridad** es parte del día a día de las personas. Para implementarla utilizamos puertas con cerraduras en casa, las distintas organizaciones controlan quién entra a sus edificios... De una forma similar el concepto de seguridad aparece en los sistemas distribuidos, los cuales podemos definir como: ün sistema en el que los componentes hardware o software están localizados en distintos dispositivos, conectado mediante una red y se comunican y coordinan mediante paso de mensajes"[5]. El hecho de que se empleen se comuniquen mediante una red es su principal problema en lo respectivo a seguridad (dejando de lado problemas con el hardware, como establecer la sincronización...)

La cuestión principal a resolver en este campo es: ¿Cómo podemos comunicar estas distintas partes asegurando que no escucha nadie más y que la información no ha sido modificada? Es decir, queremos asegurar la **confidencialidad** y la **integridad**, junto con otros problemas como el **denial of service** (a través del envío de muchas peticiones, saturar el servicio de forma que deje de satisfacer las necesidades de los clientes), relacionado con la disponibilidad.

Históricamente podemos ver muchos ejemplos de grandes fallos de seguridad como **Wannacry (2017)** causando pérdidas por valor de 4000 millones de dólares, **Stuxnet (2010)** que atacó a centrales nucleares... A continuación se detallarán algunas de las principales tendencias para la implementación de seguridad en este tipo de sistemas.

4. Descripción

Para poder establecer una visión más clara sobre los problemas que trata de resolverse a través de la seguridad, vamos a establecer sus definiciones básicas:

Confidencialidad. Propiedad por la que la información sólo puede ser accedida por las partes autorizadas para ello.

Integridad. Propiedad por la que un usuario externo es incapaz de alterar la información que dos partes de un sistema distribuido se envían.

Disponibilidad. Esta propiedad debe ser protegida por la seguridad. La definimos como la capacidad que tiene un servicio para mantenerse activo. Esta puede verse afectada por los ataques de denial of service a los que hemos hecho referencia anteriormente.

La implementación de seguridad se hace mediante políticas de seguridad, que indican para cada entidad de un sistema distribuido qué pueden y qué no pueden/deben hacer.[11]

5. Análisis

5.1. Principales técnicas de seguridad

A la hora de lograr esta seguridad mencionada, hoy día se utilizan muchos mecanismos a la hora de lograr esta seguridad en la compartición de información, tales como: [1]

5.1.1. Criptografía

La encriptación es el proceso de codificar un mensaje de manera que su contenido quede oculto, para ello existen distintos algoritmos basados en el uso de claves secretas. Actualmente, hay dos tipos principales de algoritmos de encriptación: Uno hace uso de claves secretas compartidas (el emisor y el receptor son los únicos que conocen la clave) y el otro hace uso de parejas de claves públicas y privadas (el emisor encripta su mensaje con la clave pública del receptor y el receptor desencripta el mensaje con la clave privada correspondiente del emisor).

La criptografía tres roles principales en cuanto a la implementación de sistemas seguros, los cuales detallaremos a continuación:

- **Confidencialidad e Integridad**: Mediante el uso de claves secretas descritas anteriormente, podemos asegurar que la información solo podrá ser descifrada por el destinatario, siempre y cuando las claves secretas no hayan sido comprometidas.
- **Autenticación**: Para verificar la autenticidad de los mensajes se suele tener una entidad intermediaria que verifique las claves
- **Firmas digitales**: asdf

5.1.2. Certificados

También conocido como infraestructura de clave pública, es una técnica de seguridad en la que se utiliza un sistema de certificados digitales para garantizar la autenticidad y la integridad de la información transmitida en un sistema distribuido.

La PKI integra los certificados digitales, la criptografía de clave pública y las autoridades de certificación en una arquitectura de seguridad completa.

Los principales componentes de una PKI son la política y prácticas, la autoridad de certificación (CA), la autoridad de registro (RA), aplicaciones habilitadas por la PKI y el sistema de distribución de certificados.

En un entorno de PKI, se utilizan dos claves criptográficas diferentes para el cifrado y descifrado de datos: una clave pública, que se puede compartir y distribuir, y una clave privada, que se mantiene en secreto.[9]

- La CA emite y gestiona los certificados digitales, que contienen la clave pública de la persona y otra información.
- La RA verifica la identidad del usuario y transmite las solicitudes válidas a la CA.

5.1.3. Accesos de control

Es un método que permite garantizar que los usuarios prueben ser quienes dicen que son. Es como cuando en algún lugar debes mostrar tu documento de identidad para comprobar que efectivamente tienes dicha identidad. Algunos tipos de control de acceso son los siguientes:

- **Control de Acceso basado en Roles (RBAC)**: Se basa en la concesión de acceso a los usuarios en base a los roles asignados. Además, y para añadir capas extras de protección, se aplican políticas de seguridad que limitan la obtención de privilegios.
- **Control de Acceso Discrecional (DAC)**: Es un tipo de control de acceso que dicta que el dueño de los datos decide respecto a los accesos. El responsable de ese objeto es quien va a determinar quién puede o no entrar y con qué permisos.
- **Control de Acceso Obligatorio (MAC)**: Se basa en que a los usuarios se les concede el acceso en base a regulaciones establecidas por una autoridad central en una empresa o alguna otra organización reguladora.
- **Control de Acceso basado en Atributos (ABAC)**: La distinción de este tipo de control de acceso, es que al usuario y los recursos a los cuales le corresponde el acceso, se le agregan una serie de atributos y permiten que se realicen evaluaciones que indican respecto al día, la hora, la ubicación y otros datos.

[6]

5.1.4. Firewalls

Un firewall es un sistema de seguridad de red de los ordenadores que restringe el tráfico de paquetes entrante, saliente o dentro de una red privada.

Este software o esta unidad de hardware y software dedicados funciona bloqueando o permitiendo los paquetes de datos de forma selectiva. Normalmente, su finalidad es ayudar a prevenir la actividad maliciosa y evitar que cualquier persona (dentro o fuera de la red privada) pueda realizar actividades no autorizadas.[7]

5.1.5. Sistemas de detección de intrusos (SDI)

Un sistema de detección de intrusos analiza el tráfico de red o el uso de dispositivos conectados a esa red en busca de actividades sospechosas, que o bien compara con las firmas de amenazas que tiene en su base de datos, o bien busca comportamientos anómalos respecto al funcionamiento habitual de la red o dispositivos.

Si el SDI detecta una amenaza o un comportamiento anómalo, emite una alerta para que los administradores del sistema tomen las acciones que estimen oportunas. En ese sentido, el IDS no bloquea o evita el ataque, pero sí ayuda a identificarlo cuando ocurre y lleva a tomar las medidas necesarias para mitigarlo. Como ejemplo, si el sistema observa que hay una máquina haciendo una gran cantidad de peticiones en un intento de denial of service, avisará al administrador para que bloquee sus peticiones mediante firewall o lo bloquea directamente y avisa al administrador para que tome cartas en el asunto.

La implementación de IDS puede resultar beneficiosa para una empresa ya que:

- Supervisa el funcionamiento del router, el cortafuegos, los servidores clave y los archivos.
- Garantiza una detección rápida y eficaz de las anomalías conocidas bajo riesgo de dar falsas alarmas mediante el uso de la base de datos de firmas.
- Analiza diferentes tipos de ataques, identifica patrones de contenido malicioso y ayuda a los administradores a afinar, organizar y aplicar controles eficaces.
- Ayuda a la empresa a el cumplimiento de la normativa y a satisfacer las regulaciones de seguridad.

[3][8]

5.1.6. Blockchain

Blockchain es un tipo de base de datos que almacena datos de forma segura en bloques. Conecta los bloques mediante criptografía. Blockchain permite recopilar información, pero no editarla ni eliminarla.

Los profesionales de la ciberseguridad pueden usar blockchain para proteger sistemas o dispositivos, crear protocolos de seguridad estándar y hacer que sea casi imposible que los piratas informáticos penetren en las bases de datos.

Los beneficios de blockchain incluyen una mejor privacidad del usuario, reducción de errores humanos, mayor transparencia y ahorro de costos al eliminar la necesidad de verificación de terceros.

Blockchain también elimina el problema de seguridad de almacenar datos en un solo lugar. En cambio, los datos se almacenan en las redes, lo que da como resultado un sistema descentralizado que es menos vulnerable a ataques.

Los desafíos de usar blockchain incluyen el costo y la ineficiencia de la tecnología.

5.2. Principales problemas de la seguridad

A pesar de que como hemos visto anteriormente la seguridad es un tema fundamental, estos requisitos llevan a una serie de inconvenientes.

5.2.1. Mayor Complejidad

La mayoría de las medidas de seguridad que se aplican y se implementan aumentan la complejidad del sistema ya que para esto es necesario añadir complementos de código, infraestructura o componentes, además es necesario llevar un control muy completo sobre el mantenimiento y la actualización sobre los sistemas de seguridad ya que podemos ver como el número de vulnerabilidades crece y se crean nuevos métodos y técnicas, esto implica una gran inversión en crear un sistema robusto libre del mayor número de amenazas posibles, para ello podemos seguir técnicas adecuadas como “logical proofs” y utilizar estándares ampliamente usados y revisados lo cual es muy útil a la hora de detectar fallas.

5.2.2. Tiempo latencia

Encontramos un incremento en el tiempo de latencia, es decir, la necesidad de cifrado y autenticación provoca invertir tiempo en realizar cómputos adicionales lo cual implica un deterioro en el rendimiento del sistema. Por ejemplo, si queremos proteger ciertos datos en una comunicación, tendremos que cifrar y descifrar los datos en los extremos pertinentes; el uso de algoritmos de cifrado más rápidos y eficientes será un factor crítico en el impacto del sistema.[2]

5.2.3. Menor privacidad real

El empleo de técnicas como sistemas de detección de intrusos u otros mecanismos que monitorizan la red y la distinta información que intercambian las partes hace que el usuario tenga menos privacidad ya que existe una entidad autorizada para ver toda su información (aunque tenga que cumplir siempre unos principios éticos) en pro de la seguridad.

5.2.4. Transparencia en los sistemas

Cuando el objetivo realizar un sistema los mas transparente posible, es decir, que todas las necesidades que se se realicen con la mínima interacción posible con el usuario, la seguridad implica realizar acciones que la mayoría de usuarios no se encuentran cómodos realizando, por ejemplo el uso de técnicas un poco más avanzadas a la hora de protección de datos y contraseñas, uso de dispositivos secundarios para la autenticación, 2FA.

5.2.5. Computación cuántica

La base de la criptografía actual es que tomaría mucho tiempo descifrar cualquiera de las claves generadas. Este dejará de ser un problema difícil para los ordenadores cuánticos, los cuales son capaces de hacer billones de operaciones por segundo frente a los millones que es capaz de hacer un ordenador actual.[10]

6. Conclusiones

Como es obvio, la seguridad es una parte fundamental de los sistemas distribuidos, ya que sin ella habría muchos casos de usos que no se podrían dar debido a la posibilidad de ataques y fallos (nadie utilizaría aplicaciones bancarias si fuese fácil que una persona se metiese en tu cuenta y se transfiera todo el dinero) y no se habría podido desarrollar al nivel de hoy en día. Cuando se desarrollan nuevas tecnologías y formas de sistemas distribuidos siempre se tiene en cuenta la dimensión de seguridad en este y como poder cumplir ciertos requisitos mínimos.

A pesar de sus desventajas, cada día la programación de aplicaciones distribuidas se esfuerza más por abstraer al usuario final de las cuestiones de seguridad interna, por lo que el problema de la menor transparencia es cada día menor. Además, el usuario también es consciente de que estos pasos extra que tiene que dar para acceder a una funcionalidad son en aras de su seguridad, por lo que tampoco le da extremada importancia.

Respecto a la mayor complejidad de dichas aplicaciones y de cómo actualizar ciertos protocolos de seguridad en estas, existen una gran variedad de middlewares que también se ocupan de ciertas partes de la seguridad (por ejemplo el denial of service se debe ocupar el propio servidor) y abstraen al programador de este tipo de problemas.

Es cierto que al ser más complejos los mecanismos de seguridad pueden dar un mayor tiempo de latencia, esto se trata de paliar mediante el avance en prestaciones que dan hoy en día los dispositivos además de las mejoras algorítmicas que se hacen de estos protocolos sobre todo en el campo de la criptografía, muy estudiado en la actualidad.[4]

Sin embargo, el mayor de los problemas en el ámbito de seguridad se plantea en el futuro con la computación cuántica. A pesar de que todavía no hay ordenadores cuánticos suficientemente estables

como para su uso contra la seguridad, se llevan investigando posibles soluciones desde principios de 2010 existiendo ya varios mecanismos expuestos en el artículo "Cybersecurity in the quantum era" - Petros Wallden y Elham Kashefi.

7. Autoevaluación

Este proyecto ha sido realizado siguiendo las indicaciones sobre trabajos en equipos analíticos que nos han sido proporcionados. Sin embargo, también nos hemos proporcionado apoyo entre los distintos miembros del equipo, consiguiendo una gran consonancia en el nivel de entrega máximo de cada uno de los integrantes en la realización del proyecto.

Referencias

[1] Universidad de Alcalá. *La Seguridad en Sistemas Distribuidos*. 2019.

[2] Mike Yablonowitz y Jan Jürjens Ashish Gehani. "Latency Analysis of Security Mechanisms in Distributed Systems". En: (2006).

[3] Grupo Ático34. *Sistema de detección de intrusos*. 2020.

[4] Konstantin Beznosov. *Middleware and Web Services Security*. 2004.

[5] G. Coulouris. *Distributed Systems: Concepts and Design (5th Edition)*. 2012.

[6] Lorena Fernández. *Control de accesos*. 2021.

[7] Karpersky. *Firewall*. 2018.

[8] Tech2Business. *Beneficios de un Sistema de Prevención/Detección de Intrusos*. 2019.

[9] Uanataca. *Qué es una PKI*. 2021.

[10] Petros Wallden y Elham Kashefi. "Cyber Security in the Quantum Era". En: (2019).

[11] University Of Waterloo. *Module 9: Security*. 2012.