Engineer

control de acceso

permitir o denegar cada solicitud de uso de un recurso

Qué es

El control de acceso es la parte de un sistema que responde muchas veces por segundo a una pregunta: ¿puede este solicitante realizar esta acción sobre este recurso ahora mismo? El solicitante puede ser una persona, un servicio o una tarea programada. El recurso puede ser un archivo, una fila de base de datos, un endpoint de API, un repositorio Git o una puerta. Los mecanismos concretos que responden se llaman controles de acceso, y el glosario de NIST incluye la autorización como sinónimo del concepto completo. Sus definiciones, traducidas aquí, abarcan ambas mitades de la tarea: «la decisión de permitir o denegar a un sujeto el acceso a objetos del sistema» y «el proceso de conceder o denegar solicitudes concretas» para obtener y utilizar información y servicios de procesamiento relacionados, o para entrar en determinadas instalaciones físicas.

Es fácil confundirlo con la autenticación, pero son pasos distintos. NIST SP 800-162 lo dice expresamente: «La autenticación no es lo mismo que el control de acceso». La autenticación establece quién pregunta. El control de acceso toma esa identidad y todo lo demás que se sabe de la solicitud y decide qué puede hacer quien llama. Un sistema puede verificar perfectamente a una persona y aun así dejarle leer registros ajenos porque nunca se hizo la segunda pregunta.

La misma guía divide el trabajo en dos. Un punto de decisión de políticas calcula la respuesta y un punto de aplicación de políticas se sitúa en la ruta de la solicitud y la hace cumplir. Ambos pueden residir en un mismo proceso, pero conviene recordar la separación: una decisión que nada hace cumplir no protege nada. NIST SP 800-53 lo concreta en dos controles: AC-24 exige aplicar las decisiones a cada solicitud de acceso antes de hacerlas cumplir, y AC-3 exige hacer cumplir las autorizaciones aprobadas.

Las reglas pueden adoptar varias formas: una lista de identidades permitidas en cada objeto, roles como en RBAC o atributos de quien llama, del objeto, de la acción y del entorno, que es el tema de SP 800-162. Sea cual sea la forma, algo debe plantear la pregunta en cada solicitud.

Utilice el concepto en una decisión

Aplique «¿Qué es el control de acceso?» a una decisión real. Podemos ayudarle a relacionar el concepto con el sistema que está construyendo o comprando. Cuentas, contraseñas y permisos organizados para que cada persona tenga exactamente el acceso que necesita y lo pierda el mismo día que deja la empresa.

Explore nuestros servicios Póngase en contacto →

Compruebe los supuestos detrás del término

Utilice la explicación y los trabajos enlazados para formular preguntas sobre su proyecto. Podemos examinar los supuestos con usted antes de elegir una herramienta. 1.000 reglas RBAC para servidores Linux — 1,000 reglas de acceso escritas para cerrar una brecha de seguridad

1.000 reglas RBAC para servidores Linux Póngase en contacto →

Por qué importa

Una vez iniciada la sesión, el control de acceso decide casi todo lo que alguien puede alcanzar. Una autenticación sólida delante de un control débil solo registra qué cuenta se llevó los datos. Para un negocio que conserva información ajena, aquí es donde se cumple o se rompe la promesa de quién ve qué.

NIST describe el mecanismo ideal de aplicación como un monitor de referencia. El control AC-25 de SP 800-53 exige que sea inviolable, se invoque siempre y sea lo bastante pequeño para analizarlo y probarlo. Las tres propiedades sirven como prueba práctica de cualquier control en un producto real. Si quien llama puede alterar los datos de entrada de la comprobación, falla la primera. Si una ruta llega a los datos sin pasar por ella, falla la segunda. Si la lógica se dispersa entre cientos de manejadores y nadie puede leerla completa, falla la tercera.

Application Security Verification Standard de OWASP lo convierte en requisitos comprobables por un equipo. Su capítulo de autorización exige limitar el acceso a funciones a quienes tengan permiso explícito, limitar de igual forma el acceso a datos concretos y aplicar las reglas en una capa de servicio fiable, sin depender de nada manipulable por un cliente no fiable, como JavaScript en el navegador. También exige que los cambios en los valores de los que depende una decisión surtan efecto de inmediato y, si no es posible, que un control mitigador alerte cuando alguien actúe tras perder el derecho.

La contrapartida es el coste en la ruta de la solicitud. Cada decisión necesita hechos y cada hecho una consulta. Saltarse esa consulta suele trasladar la comprobación al lugar más barato, a menudo el que controla quien llama.

Cómo se aplica en la práctica

En una plataforma marítima donde una persona puede actuar por varias organizaciones, la pregunta de quién decide se resolvió mediante el lugar de decisión: la organización activa se conserva en el cliente y nada de ello se considera fiable para decidir el acceso. Un OrganizationContext almacena la elección actual en localStorage para que el cambio sea inmediato, y una cookie del servidor la refleja para que las páginas renderizadas en él resuelvan el mismo contexto. La autorización se vuelve a comprobar en el servidor en cada solicitud. La página marca el límite en una frase: solo el servidor decide qué está permitido, y manipular localStorage cambia únicamente lo que muestra la propia interfaz, porque el servidor sigue diciendo no.

En el mismo tipo de plataforma, cobrar y conceder permisos se construyeron como dos sistemas. Las tarjetas mediante Stripe y las compras integradas de Apple y Google convergen en un esquema de pagos de 9 tablas y 34 funciones. Un esquema de acceso separado de 11 tablas y 34 funciones responde si la cuenta puede hacer algo sin conocer qué tienda cobró. Esa respuesta controla el directorio de empresas, la búsqueda y la exportación de datos, y se revisa en el servidor en cada solicitud: ocultar un botón es una cortesía, no un control. Añadir una tienda solo afecta ahora a pagos, y una consulta de soporte sobre acceso tiene una tabla que examinar en vez de tres. La página nombra el coste: dos esquemas y una consulta de derechos en solicitudes que de otro modo no la necesitarían.

Cuando la empresa trasladó el código fuente a su propio hardware, la forja Git se configuró para denegar de forma predeterminada. La página incluye el control de acceso entre las tareas de operar una forja. Se eligió una sin interfaz web administrativa: cuanta menos interfaz, menos que defender. La política parte de denegar: quien carece de identidad no obtiene nada, quien carece de clave no obtiene nada y cada repositorio declarado lleva el indicador de privado. El secreto depende así de la política, no de la oscuridad. La accesibilidad de red forma parte de ella. El puerto 23231 responde solo en loopback, lo que convierte un servidor de salto en la única entrada exterior. El multiplexor que podría exponer Git en el puerto público está en el código con el interruptor apagado: un punto de escucha que nadie usa es superficie de ataque.

Dónde surgen los problemas

La comprobación vive en la interfaz. Se oculta o deshabilita un botón y el endpoint responde a cualquiera que lo invoque directamente. El servidor debe decidir de nuevo en cada solicitud, a partir de hechos que quien llama no pueda editar.

Se comprueba la función, pero no el registro. Una solicitud identifica una factura, un documento o una cuenta; el servidor confirma que quien llama puede ver facturas y devuelve la solicitada sin comprobar a quién pertenece. ASVS llama a esta brecha referencia directa insegura a objetos (IDOR) o autorización defectuosa a nivel de objeto (BOLA). Quien defiende el sistema la reconoce por un identificador incluido en una solicitud que el servidor utiliza tal como lo recibe. La solución es resolver cada objeto dentro del ámbito de quien llama y, en un producto con varias organizaciones cliente, obtener la organización de la sesión del servidor y nunca de la solicitud.

Todo lo nuevo queda abierto hasta que alguien lo cierra. Una ruta, tabla o repositorio nuevo hereda la opción predeterminada. Si esta permite, la brecha permanece hasta que alguien la detecta. SP 800-53 expresa la regla opuesta para la red: denegar de forma predeterminada y permitir por excepción. Sirve en cada capa: lo nunca concedido se deniega.

Los permisos solo crecen. SP 800-162 señala que, si no se retiran o revocan accesos con el tiempo, los usuarios acumulan privilegios. Las personas cambian de equipo, los proyectos terminan y los contratistas se marchan; cada caso exige retirar algo. Una revocación que solo entra en vigor al caducar la sesión horas después es una versión más suave de la misma brecha.

Nadie puede explicar por qué se permitió una solicitud. Si las decisiones se toman en muchos lugares y no se registran en ninguno, no hay nada que leer al investigar. Registre concesiones y denegaciones con la regla que las produjo y proteja ese registro: SP 800-162 advierte que el patrón de decisiones puede revelar atributos de las personas detrás de las solicitudes.

Lecturas adicionales

- Control de acceso en el glosario CSRC de NIST — definiciones de FIPS 201-3 y CNSSI 4009, con autorización como sinónimo.

- NIST SP 800-53 Rev. 5 — la familia de controles de acceso, incluidos AC-3 para aplicación, AC-24 para decisiones y AC-25.
- NIST SP 800-162 — control de acceso basado en atributos, con puntos de decisión y de aplicación de políticas.
- Application Security Verification Standard de OWASP — requisitos de autorización comprobables por función, dato y campo.

Glosario

Elija según sus restricciones reales

Describa la ruta de despliegue, los riesgos operativos y quiénes se encargan de las guardias. Podemos definir el alcance de un cambio con comprobaciones, una vía de recuperación y responsabilidades claras.

Vea cuánto cuesta Póngase en contacto →

Haga práctica la terminología

Pregunte cómo se aplica «¿Qué es el control de acceso?» a su organización. Basta un ejemplo concreto de su sistema actual para iniciar la conversación.

Explore nuestros servicios

welcome@engineer.company +45 50 10 61 84 Copenhague, Dinamarca

Llévese esta página

Tarjeta de contacto

Creado con esmero y cariño por D.

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

Derechos de autor © 2025 – actualidad · Engineer ApS · Todos los derechos reservados.

Impreso desde https://engineer.company/es/glossary/access-control/