Recuperación de cuenta

Dean H. Saxe, ingeniero de seguridad senior, *Amazon Web Services*

Por comentarios sobre este artículo, contacte nuestro Repositorio GitHub o reporte un problema

Tabla de contenidos

Resumen

Todos los sistemas que requieren autenticación de usuarios, comparten un problema común: los usuarios son humanos. Los usuarios olvidan o pierden sus credenciales, pierden, reparan mediante una herramienta de reimagen, rompen o venden el dispositivo que tiene sus credenciales (por ej. un móvil o una laptop). El acceso a la cuenta se pierde cuando los usuarios pierden el acceso a la cuenta de correo electrónico asociada a su cuenta. En algunos sistemas, las credenciales expiran y deben ser reemitidas. El factor común es que los usuarios necesitan mecanismos alternativos para restaurar el acceso a las cuentas cuyas credenciales no están disponibles.

El presente artículo establece un marco para la evaluación de los mecanismos de recuperación de cuenta y ofrece recomendaciones para la recuperación de cuenta en ámbitos educativos, empresariales, gubernamentales y de consumo, identificando los beneficios y riesgos de los mecanismos comunes. Dada la variedad de preocupaciones que existen en las diferentes áreas - privacidad, seguridad y continuidad de acceso - el lector podrá aplicar la guía según su dominio en la materia y a su juicio para diseñar, desarrollar e implementar mecanismos de recuperación de cuenta para sus sistemas en línea. Dado el cruce entre las acciones de recuperación de cuentas y los equipos de atención al cliente, el autor recomienda enfáticamente que el lector consulte también el artículo "Administración de identidades en operaciones de atención al cliente" que se encuentra en el Cuerpo de Conocimiento de IDPro.

Terminología/Glosario

- **Propietario de la cuenta -** Una entidad que "posee" o que reclama responsabilidad sobre una cuenta. En general, una cuenta es expedida a nombre de su(s) dueño(s) o representantes, en el caso de empresas.
- **Recuperación de cuenta (RC) -** Es el proceso para devolver a un propietario el acceso a su cuenta cuando pierde, olvida o no puede proveer las credenciales de la cuenta. Esto puede realizarse en persona, de forma remota o híbrida.
- **Usurpación de cuenta -** La usurpación de cuenta es una forma de robo de identidad y fraude, por la cual terceros maliciosos logran acceder exitosamente a las credenciales de la cuenta de un usuario.[1]
- **Agente (o "agente de atención al cliente")** - La persona responsable de comunicar y resolver problemas en nombre del cliente o usuario final.

[1] Flanagan (Editor), H., (2021) "Terminología en el cuerpo de conocimiento de IDPro", *Cuerpo de conocimiento de IDPro* 1(7). doi: https://doi.org/10.55621/idpro.41

- **Credenciales -** Cualquier atributo o secreto compartido que pueda ser utilizado para autenticar a un usuario.
- **Autenticación basada en el conocimiento (KBA, por sus siglas en inglés) -** Es un método de autenticación que usa información conocida por el usuario final y por el servicio de autenticación, pero que no es necesariamente secreta.
- **Autenticación de múltiples factores (MFA, por sus siglas en inglés) -** Es un método por el cual la identidad de un usuario es validada al nivel de confianza requerido de acuerdo con una política de seguridad para un recurso que es accedido utilizando más de un factor (algo que sabes —como tu contraseña—, algo que tienes —como tu teléfono inteligente—, algo que eres —como tu huella digital—). [2]
- **Datos personales -** Los datos personales son cualquier información asociada a una persona natural identificada o identificable.[3]
- **Ingeniería social -** La ingeniería social es un método de manipulación de las personas para que divulguen información confidencial, como contraseñas e información bancaria, u otorguen acceso a sus computadoras para instalar secretamente software malicioso. [4]
- **Modelado de amenazas -** El modelado de amenazas es una técnica de análisis utilizada para ayudar a identificar amenazas, ataques, vulnerabilidades y contraataques que puedan impactar en la aplicación o en el proceso.[5]
- **Nombre de usuario -** Es un identificador único del servicio de autenticación que se usa en conjunto con un secreto compartido para autenticar a un usuario.

Recuperación de cuenta

Definiendo la RC

¿Qué es la recuperación de cuenta? Si bien se ofrece una definición más arriba, a continuación, encontrará una descripción más amplia. La RC es un mecanismo o conjunto de mecanismos que se utilizan para mantener la continuidad de acceso en los servicios del usuario. La RC funciona proveyendo un *mecanismo alternativo de autenticación para restablecer las credenciales de autenticación*, como por ejemplo re-identificando al usuario. Una propiedad clave de cualquier mecanismo de RC es que debe alcanzar o superar la seguridad del mecanismo de autenticación nominal para la cuenta que quiere recuperar. Si esta propiedad no se cumple, los usuarios podrían elegir ejecutar un mecanismo de RC antes que recordar sus credenciales. Esto también abre la puerta para que la RC se utilice como mecanismo de usurpación de cuenta.

---

[2] Ibid.

[3] Ibid.

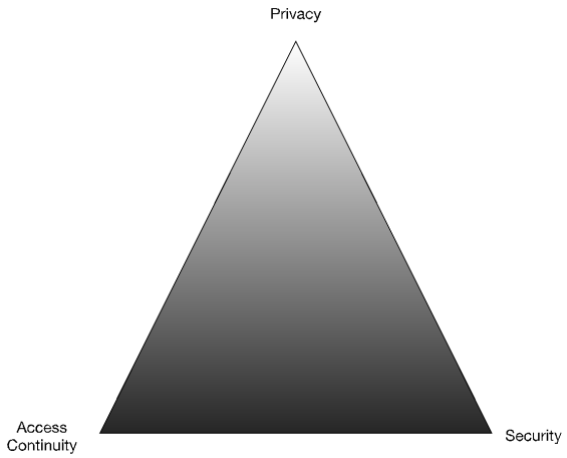
[4] Ibid.

[5] Ibid.

Un caso real del uso abusivo de mecanismos de la RC le ocurrió al propio autor de este artículo. Nuestra familia tenía acciones en una compañía estadounidense; las acciones se administraban mediante un portal en línea. Cada año tenía que iniciar sesión en el mismo para obtener los formularios de declaración de impuestos, pero yo nunca podía recordar mi contraseña. El proceso de RC del servicio requería dos piezas de información legibles: el apellido de soltera de mi suegra y la fecha de nacimiento de mi esposa. Cada año, iniciaba sesión con estas dos piezas de información, recogía los documentos que necesitaba y cerraba la sesión. ¡La contraseña no era requerida y el procedimiento de RC no solicitaba resetear la contraseña ni tampoco notificaba al propietario de la cuenta del acceso!

El triángulo de hierro de la recuperación de cuenta

Como propietario de un recurso, debo escoger un equilibrio entre estas tres preocupaciones - privacidad, continuidad de acceso y seguridad - que cubra mis necesidades dentro de las restricciones del servicio al que estoy accediendo. En un triángulo de hierro, puedo moverme de un vértice al otro para cubrir una de las preocupaciones (por ej. la seguridad) en detrimento de otra (por ej. la continuidad de acceso).[6]



En el ejemplo narrado anteriormente sobre las acciones que yo poseía en una empresa, el diseño de sistema se enfoca exclusivamente en la continuidad de acceso en detrimento de la seguridad - la cuenta es fácil de acceder por actores maliciosos que pueden ejecutar transacciones - y en la privacidad - el propietario de la cuenta es completamente identificado por el servicio ya que tal es la naturaleza de la mayoría de los sistemas financieros.

[6] Caccamese, A. & Bragantini, D. (2012). “Más allá del triángulo de hierro: año cero”. Artículo presentado en el congreso mundial de PMI® del año 2012—EMEA, Marsella, Francia. *Newtown Square*, *PA: Project Management Institute*, https://www.pmi.org/learning/library/beyond-iron-triangle-year-zero-6381

Por oposición, mi banco actual se enfoca en la continuidad de acceso y en la seguridad - es difícil obtener acceso a mi cuenta en línea gracias a los sólidos requerimientos de autenticación - y es (relativamente) fácil para mí recuperar el acceso a mi cuenta ya que solo debo presentarme personalmente en una sucursal del banco con mi documento de identidad emitido por el gobierno. El banco está obligado a identificarme basándose en mi documento de identidad emitido por el gobierno (por ej. un pasaporte, una licencia de conducir) para realizar determinadas transacciones y, en caso de que sea necesario, utiliza este mismo sistema de autenticación presencial mediante mi credencial emitida por el gobierno para restaurar el acceso a mi cuenta. *¡Esto es un acto de autenticación!* La licencia de conducir se ve normal, inalterada, los elementos anti-fraude están en orden, la fecha de vencimiento es válida, la foto se ve igual a la persona que la está presentando, el documento posee un código que es legible automáticamente por una computadora y coincide con la persona, etc.; por consiguiente, puedo realizar la transacción. (Nótese que este mecanismo de autenticación no está exento de fraude. Sin embargo, los riesgos de que un ataque se escale al mundo físico son considerablemente inferiores que en los servicios únicamente en línea).

Por último, Reddit, una red social de noticias, equilibra las tres preocupaciones. Mi correo electrónico es validado al iniciar sesión obligándome a cerrar el bucle haciendo clic en una URL de un solo uso. Reddit me permite usar múltiples dispositivos de autenticación de múltiples factores (MFA, por sus siglas en inglés) y puedo recuperar mi cuenta mediante un código de respaldo. Pero si los códigos de respaldo se pierden, se desconoce la contraseña y los dispositivos de MFA no están disponibles, perderé el acceso a mi cuenta para siempre.

¿Cuál de estas formas es la correcta? Potencialmente todas, dependiendo del modelo de amenazas.

Dadas estas limitaciones, ¿cómo podemos aplicar este triángulo de hierro para diseñar sistemas de registro, autenticación y recuperación de cuenta? Debajo encontrará tres *continuums* que representan cada vértice; el movimiento de la flecha se correlaciona con un puntaje más alto en el *continuum* hacia el vértice del triángulo (los valores son relativos, no absolutos).

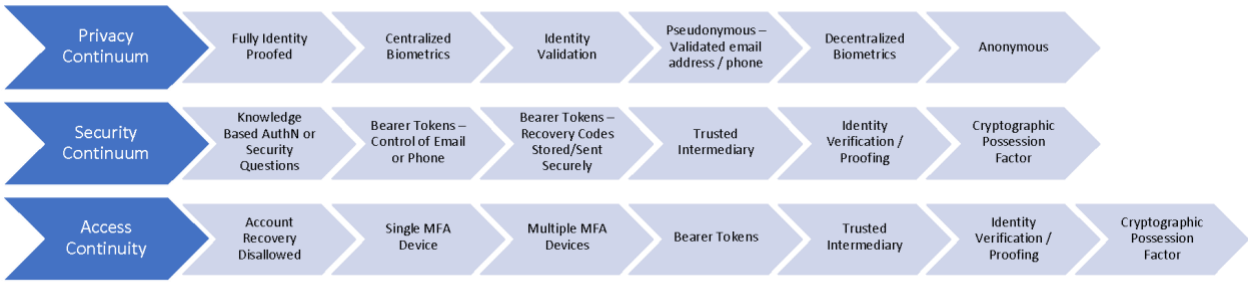


Figura 2: Los tres continuums del triángulo de hierro de la continuidad de acceso. El movimiento de izquierda a derecha dentro de cada continuum, aproxima hacia cada vértice del triángulo.

En pocas palabras, los arquitectos de identidad pueden utilizar el triángulo de hierro en primer lugar para identificar en qué parte del triángulo se sitúa el caso de uso y segundo lugar para identificar los cambios que deben hacerse para cubrir las necesidades del caso de uso. Sin embargo y como los detalles lo son todo, los mismos pueden diferir mucho entre los ecosistemas de identidad.

RC de consumidor

Los casos de uso de consumidor se centran en los usuarios finales de sistemas comerciales abiertos al público en general. Dependiendo de la naturaleza del vínculo con el consumidor pueden existir o no interacciones en persona, lo cual limita los mecanismos para restablecer las credenciales del usuario.

El riesgo asociado a las cuentas de consumidor varía ampliamente de servicio en servicio. Si bien tanto los sitios bancarios como sociales necesitan poder ejecutar mecanismos de RC para sus usuarios, el riesgo asociado a cada tipo de cuenta es significativamente diferente. A su vez, también difiere el conjunto de información disponible para habilitar la RC en diferentes servicios al consumidor. .

RC de Empresa

En una empresa, el foco de los procesos de RC está generalmente puesto en la continuidad de acceso - minimizando el tiempo de inactividad - y en la seguridad. Típicamente, la RC es directa para los empleados de planta: implica que la persona se presente con su documento de identidad emitido por el gobierno o por la empresa ante el servicio de asistencia técnica TI quien resetea las credenciales del empleado. Esta es una forma de demostración de identidad para la RC. No obstante, y dado que cada vez más empleados corporativos trabajan de forma remota, este mecanismo presencial puede no servir. En estos casos, las empresas deben buscar mecanismos remotos lo cual incluye mecanismos de demostración de identidad remotos mediante intermediarios confiables (por ej. un

supervisor) que avalen al empleado y/o mediante un quórum de intermediarios confiables que avalen al empleado, etc.

RC de educación

Al igual que en las empresas, el foco en la educación está puesto en la continuidad de acceso. El personal del campus y los estudiantes pueden usar servicios presenciales para la recuperación de cuenta. En el caso de empleados y estudiantes remotos, las instituciones educativas pueden utilizar mecanismos remotos similares a los de las empresas, adaptados a su ambiente específico.

RC de gobierno

Dada la amplia gama de variaciones que existen entre los sistemas y servicios gubernamentales, hay poca consistencia en este ámbito. Quienes implementen los sistemas de RC deberán tener en cuenta las leyes y regulaciones locales, nacionales y supranacionales, así como las normas culturales.

Mecanismos de RC

A continuación, repasaremos los mecanismos de RC más comunes. Dicho esto, sería negligente de nuestra parte no incluir el mecanismo primario: el de *dificultar la pérdida de acceso*. En otras palabras, si no comenzamos por enfocarnos en mantener la continuidad de acceso de nuestros usuarios, tendremos más solicitudes de RC. **Los arquitectos de identidad deben considerar los casos de RC como una preocupación primaria al diseñar sistemas de autenticación y no tratar la RC como casos de segunda clase.**

Dificultar la pérdida de acceso

¿Cómo hacen los servicios para que la continuidad de acceso sea fácil y la pérdida del acceso, difícil? En el nivel más básico, los servicios deberían alentar a sus usuarios a que tomen buenas decisiones. Esto incluye:

- Establecer el punto de partida de la información de contacto: ¿El usuario tiene acceso a su correo electrónico, móvil u otra vía de contacto? En caso negativo, ¿Existe algún tipo de mecanismo de respaldo para contactar al usuario? ¿Tu sistema de identidad cerró el bucle al completar el registro de la cuenta garantizando el acceso a información básica de contacto?

- Establecer el punto de partida de los mecanismos de autenticación: Tus usuarios pueden tener uno o más dispositivos para autenticarse ante diferentes servicios. ¿Los usuarios pueden acceder a mecanismos de autenticación como autenticadores FIDO, autenticación con contraseña de un solo uso (OTP por sus siglas en inglés) o un número de teléfono para recibir SMS? ¿Siguen en pie estos dispositivos o mecanismos?

- Autenticación de respaldo: ¿Cómo se autentican los usuarios en caso de que el autenticador primario no esté disponible? Un ejemplo común es el de un usuario que está viajando - tiene acceso a Internet, pero puede no poder recibir SMS. ¿Cómo se autentica el usuario si el servicio solo requiere una autenticación con contraseña enviada por SMS? Las mejores prácticas deberían contemplar múltiples opciones de autenticación para los usuarios como múltiples OTPs, autenticadores FIDO y códigos de respaldo. La pérdida de una no desencadena un evento de RC ni limita la disponibilidad del servicio. Limitar a los usuarios a un único mecanismo de MFA *garantiza* que ese usuario se verá obligado a ejecutar una RC si el dispositivo se pierde, rompe o está temporalmente no-disponible. *¡Esta es una experiencia de usuario que debe evitarse!*

- Recordarles a los usuarios que establezcan uno o más mecanismos de RC al inicio del ciclo de vida de una cuenta y alentarlos a actualizar regularmente estos mecanismos. Los usuarios que no tengan un mecanismo de recuperación de cuenta corren el riesgo de no poder recuperarla nunca más. Si el usuario no configuró una RC, utilice los cambios significativos (por ej. aumento extraordinario en el uso de un servicio en la nube), los chequeos de seguridad o use otros instrumentos para incentivar al usuario .

Los proveedores de identidad también deberían guiar a sus usuarios para evitar los puntos únicos de fallo de su lado. Por ejemplo, si el usuario guarda sus credenciales en un gestor de contraseñas y sus códigos de recuperación se encuentran en el mismo lugar, la pérdida de acceso al gestor de contraseñas elimina una de las posibles vías de recuperación. Si bien no siempre podemos prevenir que los usuarios caven su propia fosa, sí podemos intentar reducir el daño que se puedan hacer a sí mismos.

Notificaciones de usuario

Antes de adentrarnos en los mecanismos de la RC, debemos hablar de las notificaciones de usuario ya que son un componente importante de la experiencia de usuario en los procesos de RC. Todas las acciones que impacten la continuidad de acceso del usuario, se le deben reportar. Estas incluyen, pero no se limitan a:

- Cambios en la dirección de correo electrónico asociada a la cuenta
- Cambios en el número de móvil asociado a la cuenta
- Cambios en las credenciales de la cuenta, incluyendo, pero no limitado a:
    - Contraseñas
    - Dispositivos o mecanismos MFA
    - Reseteo o re-emisión de los códigos de recuperación
- Eliminación o incorporación de intermediarios confiables
- Recuperación de cuenta (exitosa o fallida)

Dada la premura de estos mensajes, los mismos deberían ser enviados a todos los canales disponibles que el usuario haya proporcionado como el correo electrónico, SMS y notificaciones *push*. Las notificaciones deberían enviarse al correo electrónico y/o al móvil durante una solicitud de cambio, dando al usuario la posibilidad de identificar un cambio fraudulento y revertirlo antes de que el daño sea mayor.

Tokens al portador

Los tokens al portador (en inglés *Bearer Token*), utilizados para la RC, son como el ticket o la entrada en papel que uno presenta para ingresar a un concierto o a un evento deportivo. Los tokens al portador se utilizan una sola vez para acceder a un servicio en lugar de las credenciales normales del usuario.

Estos tokens al portador toman diferentes formas:

- Códigos alfanuméricos enviados por correo electrónico o SMS en respuesta a una solicitud de RC.
- Enlaces mágicos, una forma de iniciar sesión sin contraseña, que se envían por correo electrónico o SMS en respuesta a una solicitud de RC.
- Códigos de recuperación obtenidos antes de perder acceso y almacenados en copias físicas o digitales en un lugar seguro.
- Código de recuperación enviado al usuario mediante un servicio de correo postal público o privado.

Agrupar estos mecanismos bajo el nombre de tokens al portador nos permite reflexionar sobre su usabilidad y seguridad. El nivel de seguridad de un token al portador está directamente relacionado con cómo fue entregado. Los códigos de recuperación obtenidos en una sesión autenticada son mucho más seguros que los códigos de un solo uso o los enlaces mágicos; sin embargo, esto depende de cómo son almacenados por el usuario.

Beneficios

- Es una experiencia de usuario sencilla que no requiere conocimientos o hardware especializados. Luego de desencadenar un evento de RC, como por ej. introduciendo su nombre de usuario en un proceso de RC, el usuario recibe el token al portador el cual le permite restablecer sus credenciales con el servicio.

Amenazas y mitigaciones

- Los tokens al portador pueden ser utilizados por quien sea que los “porte” - esto hace que sean fáciles de usar y abusar, como por ej. a través del *phishing* (acto de engañar a un usuario para que revele información confidencial luego de ganarse su confianza).
    - Minimiza la ventana de validez de todos los tokens al portador.
    - Verifica la conservación del estado - ¿El usuario sigue en el mismo dispositivo o navegador que al momento de desencadenar la solicitud de RC? ¿Cambió la IP? Ten en cuenta cualquier otro dato que pueda recogerse para garantizar que el usuario no es víctima de *phishing*.

- Los riesgos de los tokens al portador también incluyen el riesgo del medio a través del cual son enviados al usuario. Estas amenazas no pueden ser mitigadas por el proveedor de identidad.
    - El correo electrónico es interceptado, por ej. mediante phishing, permitiendo que actores maliciosos accedan el token al portador enviado por esa vía.
    - Los SMS son interceptados, por ej. mediante la duplicación de SIM o ataques SS7.
    - Los mecanismos de correo electrónico y SMS están sujetos a amenazas contra los proveedores y sus infraestructuras.
- Los usuarios fallan en copiar los códigos de recuperación, fallan en almacenar los códigos de recuperación en un lugar seguro o pierden sus códigos de recuperación.
    - Los proveedores pueden recomendar mecanismos de almacenamiento y gestión de los códigos, pero el usuario puede no seguir la recomendación.
- Los usuarios pierden el acceso a su correo electrónico o móvil o ingresan datos incorrectos a los que no pueden acceder.
    - Verifica que el usuario tiene acceso al correo electrónico o móvil cuando los provea al IdP.
    - Comprueba la continuidad de acceso al correo electrónico o móvil a lo largo del tiempo.

Autenticación basada en el conocimiento / preguntas de seguridad

Tanto la autenticación basada en el conocimiento (KBA, por sus siglas en inglés) como las preguntas de seguridad, se utilizan como mecanismos de recuperación ya que el usuario debe “demostrar” que es el propietario legítimo respondiendo preguntas cuya respuesta solo él conoce. Desgraciadamente, tanto la KBA, basada en bases de datos de información pública o en transacciones recientes del usuario, como las preguntas de seguridad, que se basan en preguntas predeterminadas y respuestas provistas por el usuario, son mecanismos de recuperación débiles.

Los mecanismos KBA suelen utilizar información como la dirección postal, fechas o montos de préstamos e información crediticia para identificar, de forma débil, al humano propietario de una cuenta. Sin embargo y debido a las numerosas filtraciones de datos, esta información es insuficientemente secreta y un mecanismo de recuperación no debería depender de ella para restablecer el acceso a cuentas que tengan cualquier valor significativo. De igual manera, las preguntas de seguridad suelen tener respuestas predecibles o fácilmente identificables. Las preguntas sobre el color favorito tienen baja entropía (de acuerdo con este estudio, el 64% de los estadounidenses elige uno de estos cuatro colores favoritos: azul (29%), verde (21%), violeta (8%) y rojo (8%)), mientras que las respuestas sobre el equipo deportivo favorito o mascota del secundario preferida pueden encontrarse mediante las redes sociales del usuario.

Dado que son mecanismos de baja seguridad, la KBA y las preguntas de seguridad se recomiendan únicamente para operaciones de bajo riesgo y como último recurso.

Beneficios

- La KBA y las preguntas secretas son fáciles de usar, cuando funcionan.

Amenazas y mitigaciones

- Los datos para la KBA pueden obtenerse mediante registros que se hayan filtrado o a través de bases de datos públicas
    - No utilice KBA para la recuperación de cuenta.
- Protección insuficiente en casos de violencia doméstica en los que los datos KBA pueden ser conocidos.
    - No utilice KBA para la recuperación de cuenta.
- Los clientes pueden no recordar los detalles para responder a las preguntas KBA. La imposibilidad de un cliente de recordar detalles como transacciones financieras va a desencadenar un falso negativo para un cliente legítimo. A su vez, un usuario que responda correctamente todas las preguntas podría ser un estafador.
    - No utilice KBA para la recuperación de cuenta.
- Las preguntas de seguridad y sus respuestas pueden olvidarse. Los usuarios pueden no recordar las respuestas, pueden escribir mal las respuestas, o utilizar mal las mayúsculas o puntuación, todo lo cual puede causar que el usuario falle en su autenticación.
    - Planificar las preguntas de seguridad y las respuestas para garantizar la continuidad de acceso.
- Las preguntas de seguridad y sus respuestas son contraseñas alternativas y pueden padecer los mismos riesgos que cualquier estrategia de autenticación con contraseña.
    - Para eliminar este riesgo, nunca se debe solicitar a un usuario que comparta con agentes de atención al cliente datos KBA ni preguntas de seguridad y sus respuestas.
    - Sigue la guía de almacenamiento de contraseña para todas las preguntas de seguridad y sus respuestas.

Verificación de identidad / demostración de identidad

En algunos casos de uso en los que la privacidad de la identidad del individuo no es la prioridad, los sistemas pueden usar la verificación de identidad o la demostración de identidad para establecer la identidad de un humano en el mundo real. Generalmente, esto se realiza basándose en las credenciales emitidas por una autoridad confiable como el gobierno (licencia de conducir, pasaporte), una empresa (identificación de empleado) o el sistema educativo (identificación de una universidad o colegio). La identidad del usuario es verificada al inicio del ciclo de vida de una cuenta, posiblemente como requisito para establecer la cuenta, enlazando la identidad del usuario a su cuenta. Esto puede hacerse en persona (por ej. en el banco, registrándose en un programa de viajero de confianza, en una universidad al inscribirse, en una oficina el primer día de trabajo de un empleado) o de forma remota. Dado que estos casos requieren interacciones en persona, no pueden ser

fácilmente automatizadas y por lo tanto proveen una barrera de seguridad más alta frente a accesos fraudulentos. En el caso de uso remoto, una modalidad común es solicitar al usuario que envíe una imagen de su documento de identidad y una foto o un video corto de su rostro que es típicamente usado como comprobación de vida tras solicitar al usuario que realice ciertas acciones (como mirar hacia arriba, hacia abajo, a la izquierda, a la derecha), antes de confirmar que el humano detrás de la pantalla es el mismo humano que en el documento de identidad (con cierto grado de exactitud).

Beneficios

- Vincula la persona natural al usuario de la cuenta de forma inquebrantable. Aún si el usuario reemplaza su pasaporte, la verificación de identidad puede ser ejecutada nuevamente para verificar que el humano es el "propietario" de la cuenta que está intentando recuperar (dentro de ciertos intervalos de confianza).
- Es resistente a mecanismos fraudulentos escalables, aunque esto dependerá del mecanismo específico utilizado.
- Puede ser altamente automatizado con Inteligencia Artificial/Aprendizaje Automatizado (AI/ML, por sus siglas en inglés); no obstante, muchos proveedores aún utilizan primero la revisión manual de documentos de identidad menos comunes antes de usarlos para entrenar los sistemas AI/ML.

Amenazas y mitigaciones

- Los usuarios no se sienten cómodos compartiendo sus documentos de identidad con servicios en línea. Por ejemplo, el Servicio de Impuestos Internos de Estados Unidos (IRS, por sus siglas en inglés) utiliza *ID.me* para proveer servicios de demostración de identidad en 2022, lo cual suscitó una significativa respuesta negativa.[7]
    - Ofrece información clara sobre cómo los datos provistos serán usados y almacenados.
    - Provee un mecanismo alternativo para los usuarios que no quieran o no puedan proveer documentos de identidad para la demostración de identidad remota, como por ejemplo la demostración de identidad en persona.
- Documentos fraudulentos
    - Actualmente no hay un criterio común para evaluar los servicios de verificación/demostración de documentos de identidad que compiten entre sí.
- Ataques de presentación - un tercero malicioso presenta una imagen fija o un video de la persona real a fin de realizar una verificación de identidad fraudulenta
    - Las fotos y videos *selfies* deben usar mecanismos de comprobación de vida para garantizar que son reales y que están siendo capturados en tiempo real.

[7] Thimot, Tom, "La debacle del *ID.me* de IRS: Un momento de aprendizaje para la tecnología" Venture Beat post, 15 de abril de 2022, https://venturebeat.com/2022/04/15/the-irs-id-me-debacle-a-teaching-moment-for-tech/

Intermediarios confiables

Una práctica común en el ámbito empresarial es que los usuarios recuperen el acceso mediante un intermediario confiable, como puede serlo el supervisor del usuario. El caso de uso típico es cuando un empleado pierde el acceso y necesita resetear su contraseña o configurar un nuevo dispositivo MFA. El equipo de asistencia técnica o el supervisor del usuario (o el siguiente cargo superior, aunque esto da peores resultados) puede autenticar al usuario ante un servicio de recuperación para ayudarlo a restablecer sus credenciales corporativas. Los procedimientos individuales pueden variar según el nivel de familiarización del usuario con el intermediario confiable. Por ejemplo, ante un reporte directo al supervisor este puede mediar la recuperación sin la necesidad de presentar información de identidad. El propio usuario tendrá que presentar una identificación corporativa u otra información de identidad al equipo de asistencia técnica antes de que se ejecute el reseteo de su contraseña. En el caso de empresas de servicio, un supervisor de ventas o técnico de cuentas, puede ser el intermediario confiable para los clientes que pierden el acceso. El procedimiento puede completarse en persona, por teléfono o mediante una videoconferencia.

Para crear un mecanismo de recuperación propio, Facebook utiliza un modelo de contactos confiables.

Se pueden utilizar múltiples intermediarios en un mecanismo de autenticación de quórum (*m* de un total de *n*). Los quórums son útiles para los casos de uso que requieren una mayor seguridad para eliminar las amenazas de ingeniería social o evitar los usuarios maliciosos que utilizan los procesos de RC para acceder a cuentas no autorizadas.

Beneficios

- Distribuye el trabajo de RC entre varios posibles usuarios confiables, permitiendo un mayor nivel de continuidad de acceso.

Amenazas y mitigaciones

- Los intermediarios “confiables” maliciosos toman el control de la cuenta en cuestión.
  - Solicita quórums.
  - No envíes tokens o URLs, etc., de recuperación a través de intermediarios confiables. Obliga al intermediario a enviar el token al sujeto de la acción de RC vía correo electrónico, SMS u otros mecanismos. (Pero ten cuidado, ¡esto podría parecer phishing!)

Factor de posesión

De forma similar al token al portador abordado anteriormente, el factor de posesión - como por ej. la capacidad de firmar una transacción con una clave privada específica - puede utilizarse como factor de recuperación. No obstante, no se debe esperar que el

usuario promedio genere y gestione sus propias claves de forma segura. La incorporación de claves de seguridad y *passkeys* FIDO2 generan un mecanismo seguro para la creación y gestión de pares de claves específicas de la cuenta. Al ser utilizados como un dispositivo de primer factor (por ej. flujos de autenticación sin contraseña), una clave de seguridad o un *passkey* pueden registrarse como "clave de recuperación" para la cuenta.[8] Únicamente el propietario que posea la clave junto con una acción biométrica o PIN de desbloqueo podrá recuperar la cuenta. Las aplicaciones de un dispositivo móvil pueden utilizarse como factor de posesión cuando son desbloqueadas mediante una acción biométrica o PIN de desbloqueo. Esto puede hacerse utilizando protocolos comunes como *passkeys* FIDO o por medio de un mecanismo hecho a medida.

Por último, la Identidad Auto-Soberana (SSI, por sus siglas en inglés) utiliza un mecanismo similar. Al demostrar que es el propietario de una clave privada específica asociada a su documento DID, probablemente el usuario podrá recuperar su cuenta.

Beneficios

- Facilita la RC si el factor de posesión se registra temprano en el ciclo de vida de la cuenta y puede ponerse a disposición en función de la necesidad del usuario.

Amenazas y mitigaciones

- Pérdida de la clave criptográfica o de su medio de almacenamiento.
    - Los implementadores deben tener en cuenta que la pérdida del móvil ocurre bastante frecuentemente comparado con una clave de hardware o una clave pública generada en el disco del usuario, por ejemplo. Esto puede ser mitigado mediante *passkeys* sincronizadas a través de un servicio en la nube.
    - Permite a los usuarios múltiples factores de posesión por cuenta.
    - Recuerda periódicamente a los usuarios que verifiquen su capacidad de recuperación mediante los factores de posesión.

Servicio de atención al cliente

El último mecanismo de RC es a través de un servicio de atención al cliente, como por ej. el de una empresa. Para procesar una solicitud de RC, los servicios de atención al cliente pueden utilizar uno o más de los mecanismos abordados anteriormente. Para más información sobre cómo usar el servicio de atención al cliente para la RC, vea

[8] El lector atento notará que es el mismo mecanismo propuesto por FIDO Alliance para recuperarse de la pérdida de una clave de seguridad. En esta ocasión, no hay forma de respaldar una clave de seguridad, por eso registrar múltiples claves es el mecanismo específico para la recuperación de cuenta.

“Administración de identidades en operaciones de servicios de atención al cliente”, escrito por Arynn Crow y JP Rowan.[9]

La no recuperación de cuenta

En algunos escenarios, la no recuperación de cuenta puede ser la opción más segura y una que preserve la privacidad. Si bien en la mayoría de los casos no es recomendable hacerlo, no ofrecer un mecanismo de RC puede ser la mejor opción para minimizar los riesgos de usurpación de cuenta en casos de servicios de alta seguridad.

Conclusión

La recuperación de cuenta es un mecanismo para mantener la autenticación de los usuarios en tu servicio. Para construir un servicio de RC, los propietarios del servicio deben tener en cuenta lo que ellos y sus clientes valoran: la continuidad de acceso, la seguridad o la privacidad y crear un mecanismo de RC que equilibre estos tres aspectos. A su vez, la elección de los mecanismos de RC dependerá del ámbito en el que el servicio se implementará: educativo, empresarial, gubernamental, etc. Cada uno tiene diferentes capacidades que pueden habilitar mecanismos de RC más fuertes. Dicho esto, todos los mecanismos de RC tienen algo en común: si los usuarios desean recuperar el acceso perdido a sus cuentas, deben registrarse de forma implícita o explícita para poder utilizarlos. Por eso, la RC es mucho más que una solución técnica que debe implementarse. Es un problema relacionado con la experiencia de usuario y el comportamiento humano que debe resolverse.

Agradecimientos

- Arynn Crow
- JP Rowan
- David Brossard
- Paul Figura

Biografía del autor

Dean H. Saxe es ingeniero de seguridad senior en el equipo de identidad de AWS y miembro fundador de IDPro. Se lo puede contactar en dean@thesax.es o en Twitter @n3rd1ty.

[9] Crow, A. & Rowan, J. P., (2021) “Administración de Identidades en Operaciones de Servicios de Atención al Cliente”, *Cuerpo de Conocimiento de IDPro* 1(4). doi: https://doi.org/10.55621/idpro.65.

Registro de cambios

Fecha	Cambio
03-06-2022	V2 publicada; aclaraciones incorporadas a los mecanismos de RC
19-04-2021	V1 publicada