Autenticación mediante información contextual y biometría

Los mecanismos de autenticación que se basan en contraseñas convencionales son aún los más extendidos y utilizados, pero desafortunadamente tienen un nivel de seguridad bajo y son vulnerables a múltiples ataques que facilitan la suplantación de identidad. En este sentido, las estrategias de seguridad basadas en el análisis de la información contextual y la biometría del comportamiento incrementan el nivel de seguridad que proporcionan por sí mismas las contraseñas.

Para ello, se están extendiendo los servicios de seguridad que tienen en cuenta el contexto particular en el que sucede cualquier operación. Son los llamados *context-aware security services*, que aprovechan toda la información adicional que pueda contribuir, entre otros aspectos, a mejorar la toma de decisiones de autenticación y autorización.

En el caso particular de la autenticación, el análisis de contexto aprovecha la circunstancia de que cada usuario tiene unos hábitos de comportamiento bastante estables: se conecta en determinadas franjas horarias desde puntos de acceso concretos (desde su domicilio o desde el trabajo) y usa un conjunto reducido de dispositivos (sus ordenadores y *smartphones*). Por lo tanto, cuando se conocen estos hábitos de comportamiento, es posible detectar anomalías que pueden indicar que se ha producido un intento de suplantación del usuario legítimo.

Por otra parte, en determinados entornos, tales como el corporativo, el riesgo de suplantación de los hábitos del usuario es mayor. Es decir, que el atacante, conocedor de la contraseña, pueda llegar a suplantar los hábitos del usuario y usar el dispositivo del usuario a suplantar. En este sentido la propuesta de Safelayer aporta una capa de protección adicional basada en la biometría del comportamiento, capaz de detectar el intento de suplantación de los hábitos y dispositivos.

El contexto y su captura

El contexto de autenticación del usuario está determinado por ciertas características y datos del entorno en el que se realiza el proceso de autenticación, como el dispositivo y la red de conexión, la ubicación, la información sobre la franja horaria y otros datos acerca del comportamiento del usuario. Si en sucesivas autenticaciones el contexto permanece constante o sufre variaciones razonables, podremos afirmar que la probabilidad de que el usuario autenticado sea el propietario legítimo de las credenciales es mayor que si ocurre lo contrario, es decir, si el contexto varía notablemente en diferentes procesos de autenticación. La distancia entre contextos se determina en la fase de análisis del contexto y proporciona como resultado el nivel de riesgo de la autenticación. Básicamente, a mayor distancia entre contextos, mayor riesgo de que se trate de un intento de suplantación del usuario legítimo.

La captura del contexto del usuario ocurre en diferentes momentos, a lo largo del proceso de autenticación. Una parte de la captura ocurre en el propio dispositivo del usuario, en la interfaz de aplicación donde el cliente introduce sus credenciales, y otra parte ocurre en el servidor de autenticación.

La captura y el análisis de los factores de contexto es un proceso que no afecta a la experiencia de usuario y, por lo tanto, consigue disminuir el riesgo y mejorar la seguridad de la autenticación de forma casi transparente.

La captura en el lado cliente se lleva a cabo de forma transparente mediante código que el servidor de autenticación envía de forma segura al navegador o la aplicación del usuario. Con este código se captura información del dispositivo, como el tipo y versión del navegador y del sistema operativo; características de la pantalla; el idioma y la zona horaria del dispositivo; las fuentes y plug-ins instalados, etc. Todos estos parámetros se envían de forma segura al servidor, que compone una huella del dispositivo de usuario. La huella del dispositivo podrá compararse con otras huellas de dispositivos que el mismo usuario haya utilizado en autenticaciones previas. La comparación de huellas de dispositivos sigue un algoritmo inteligente que es capaz de detectar el grado de coincidencia en función de los datos. Por ejemplo, dos huellas distintas pueden corresponder al mismo dispositivo si simplemente ha cambiado la versión del navegador; no obstante, los dispositivos se considerarán diferentes si ha cambiado el tipo de sistema operativo.

La combinación del análisis de la huella del dispositivo y la utilización de cookies de un solo uso constituye un identificador complejo de dispositivo[1], tal y como establece el organismo Federal Financial Institutions Examination Council (FFIEC) de EE.UU.

Adicionalmente, en el lado cliente también se captura la información de red, consistente en la dirección IP y próximamente de geolocalización (latitud y longitud). Esta última dependerá del tipo de dispositivo; por ejemplo, en un entorno desktop puede obtenerse de la red wi-fi, mientras que en un entorno móvil también podría obtenerse del componente GPS y/o GSM.

En el lado servidor se captura la fecha y hora de la autenticación, se vuelve a capturar la información de red y también se obtiene la geolocalización a partir de la dirección IP.

[1] *"Autenticación segura por capas. Una defensa efectiva contra el phishing y el pharming", SafelayerSecureCommunications, 2012*

El análisis de la ubicación geográfica puede apuntar situaciones de riesgo cuando se detecta el inicio de autenticaciones consecutivas desde ubicaciones demasiado alejadas geográficamente.

Opcionalmente, también se captura en el cliente información biométrica del usuario que se autentica. En concreto, para una autenticación basada en nombre de usuario y contraseña, se captura el ritmo de tecleo y se utiliza como rasgo biométrico distintivo de comportamiento. Así como ciertos parámetros del contexto se utilizan para la identificación del dispositivo, la dinámica de tecleo se utiliza para mejorar la identificación del usuario.

Toda la información recopilada interviene de forma opcional en el análisis del contexto y es el operador de la solución de autenticación quien controla qué parámetros considera más relevantes y convenientes como factores de autenticación.

Mejora de la autenticación a través de la dinámica de tecleo

Del mismo modo que cada persona genera un trazo personal y distintivo cuando escribe a mano, también presenta una serie de características que la hacen prácticamente única cuando escribe con un teclado. Esta característica se conoce como dinámica de tecleo y se trata de un rasgo biométrico que puede contribuir a fortalecer los procesos de autenticación.

La dinámica de tecleo es un rasgo biométrico relacionado con el comportamiento del usuario.

Una de las ventajas del sistema de análisis de dinámica de tecleo respecto a otros sistemas biométricos es que se trata de un mecanismo no intrusivo que puede llegar a funcionar de forma totalmente transparente para los usuarios. Por un lado, la captura de parámetros se realiza a través del teclado, de forma que no es necesario disponer de ningún sensor hardware adicional. Por otro lado, la captura se realiza desde las propias aplicaciones (por ejemplo, con código JavaScript interpretable por todos los navegadores), y por lo tanto no es necesario utilizar ningún software específico. De esta forma, el sistema de análisis de tecleo puede activarse mientras los usuarios siguen utilizando sus credenciales tal como estuvieran haciéndolo habitualmente.

El beneficio de utilizar un factor relacionado con la biometría del comportamiento es que ofrece buenas tasas de identificación con un nivel de intrusión mínimo en la experiencia del usuario. Esta característica permite detectar posibles suplantaciones de identidad, ya sean sin o con el conocimiento del usuario legítimo; en otras palabras, ya sea porque un atacante consigue robar una credencial o porque el usuario legítimo la cede a un tercero, el análisis de la dinámica de tecleo revelaría el uso indebido de la credencial.

En particular, el análisis de la dinámica de tecleo puede ser muy útil para detectar que un atacante está utilizando las credenciales de un usuario legítimo en entornos corporativos, donde es muy fácil reproducir otros factores de autenticación como el horario o la ubicación de conexión, e incluso es relativamente factible conseguir la credencial y el dispositivo de otro empleado.

TrustedX Adaptive Authentication es capaz de reconocer si la dinámica de tecleo capturada y analizada en cada proceso de autenticación que coordina, corresponde al usuario legítimo. Safelayer ha llevado a cabo el diseño y la implementación de su propio sistema de análisis.

Los parámetros que caracterizan la dinámica de tecleo de cada usuario y que se utilizan para generar su patrón biométrico son principalmente 1) el tiempo que dura la pulsación de cada tecla; 2) el tiempo que transcurre entre la pulsación de una tecla y la siguiente, y 3) el tiempo que transcurre entre la liberación de una tecla y la pulsación de la siguiente. Además, estos parámetros temporales se complementan con otros que contribuyen a definir con más precisión el patrón de tecleo del usuario. Por ejemplo, se monitoriza i) si los caracteres en mayúscula y los símbolos se realizan con las teclas SHIFT o con el bloqueo de mayúsculas; ii) si las cifras se introducen desde el bloque numérico; iii) el número de veces que se pulsa la tecla DELETE o BACKSPACE, para tener en cuenta si el usuario suele equivocarse al introducir las credenciales; iv) el uso de la tecla tabulador o del ratón para saltar entre campos del formulario, y v) el uso de ENTER o del ratón para enviar las credenciales.

El componente de análisis de dinámica de tecleo de TrustedX no necesita conocer el código de las teclas que se pulsan, por lo que su uso no compromete la confidencialidad de las contraseñas.

El aprendizaje del sistema

Para poder realizar un análisis del contexto de autenticación, el sistema debe disponer de una base de conocimiento previo acerca del comportamiento habitual del usuario. De esta forma, el sistema podrá determinar si la autenticación se está llevando a cabo en unas condiciones razonables o si se trata de una situación anómala, que apunte a una posible suplantación de identidad. Para construir esta base de conocimiento, el sistema de autenticación debe establecer las condiciones del periodo de aprendizaje.

En particular, y como en cualquier sistema biométrico, los usuarios deben superar una fase inicial de registro (también conocida como enrollment o entrenamiento) para que posteriormente pueda efectuarse el análisis de su dinámica de tecleo. En esta fase de entrenamiento, el usuario introduce varias veces sus credenciales para que el sistema pueda construir su patrón biométrico. Este proceso de entrenamiento puede ser explícito –cuando el usuario introduce repetidamente sus credenciales en una interfaz expresamente destinada al entrenamiento– o transparente –cuando el sistema va almacenando muestras de la dinámica de tecleo del usuario en sucesivas autenticaciones.

Además, tras la fase de entrenamiento, el patrón puede seguir actualizándose con las nuevas muestras capturadas durante los procesos de autenticación, ya que el usuario puede ir alterando su dinámica de tecleo a medida que se habitúa a introducir sus credenciales.

Las muestras introducidas por el usuario deben ser suficientemente similares entre ellas para que el patrón biométrico tenga una calidad mínima que garantice el correcto funcionamiento del sistema de análisis. En un proceso de entrenamiento explícito, el usuario puede ir viendo la calidad del patrón que está generado a medida que acumula

muestras. De este modo, el usuario puede descartar las muestras que empeoren la calidad del entrenamiento o incluso patrones de tecleo completos.

El sistema de análisis de dinámica de tecleo almacena el patrón de tecleo de cada uno de los usuarios. En cada acceso de un usuario, se comparan la muestra de tecleo capturada y el patrón de tecleo del usuario propietario de las credenciales introducidas. Si el grado de coincidencia de la muestra y el patrón es muy elevado, se incrementa la garantía de que el usuario que se está autenticando sea el propietario de las credenciales. Sin embargo, un nivel de coincidencia bajo entre la muestra y el patrón puede significar que el usuario que ha introducido las credenciales no es el propietario de las mismas.

Si bien la captura de la dinámica de tecleo se lleva a cabo en el mismo momento en el que se introducen las credenciales, el algoritmo de reconocimiento de dicha dinámica sólo entra en funcionamiento tras la validación de credenciales, para reforzar la autenticación. Es decir, el análisis de la dinámica de tecleo se utiliza para corroborar la identidad del usuario y verificar que no se trata de un atacante, no para identificar al usuario.

Como cada usuario puede acceder desde varios dispositivos, es posible que su patrón de tecleo sea distinto en cada uno de ellos, dependiendo de las características de cada teclado. Por este motivo, es procedente permitir que el usuario lleve a cabo la fase de entrenamiento en dispositivos distintos para poder tener en cuenta distintos patrones.

El componente de análisis de dinámica de tecleo actúa independientemente del dispositivo en el que se generó el patrón. Así, si el usuario teclea del mismo modo en varios dispositivos, probablemente no necesite hacer más de un entrenamiento.

En el caso de los smartphones y las tabletas, que disponen de pantallas táctiles, el método de captura de la dinámica de tecleo es exactamente el mismo que en los dispositivos con un teclado de sobremesa. Sin embargo, las tasas de error de los procesos de registro y análisis se ven incrementadas porque 1) los usuarios suelen usar estos dispositivos en posiciones diversas o incluso en movimiento, y 2) el tecleo es más irregular e impreciso que en un teclado de sobremesa. Por este motivo, se están investigando otros rasgos biométricos, como el reconocimiento facial o el análisis de movimientos, que resulten más cómodos de utilizar en dispositivos móviles, a la vez que mantengan el nivel de efectividad en la identificación.

El sistema biométrico de Safelayer tiene una tasa de acierto superior al 95%. La tasa de falsos negativos se minimiza gracias a la intervención de otros factores de contexto en el análisis.

El contexto y los factores de autenticación

El análisis del contexto aporta varios factores de autenticación que se suman al factor “algo que el usuario sabe”, esto es, a su contraseña. Cada uno de estos factores se puede interpretar como una capa de seguridad adicional que fortalece la contraseña y aumenta la protección del sistema:

- Algo que el usuario tiene, o el análisis del dispositivo del usuario, en el que se evalúa la probabilidad de que el dispositivo bajo análisis esté en posesión y bajo el control del usuario legítimo.

- Algo que el usuario hace, o el análisis de la ubicación y franja horaria habitual del usuario legítimo.
- Algo que el usuario es, o el análisis biométrico de la dinámica de tecleo del usuario legítimo.

Adicionalmente al análisis individual de cada uno de los factores anteriores, se puede llevar a cabo un análisis cruzado en forma de correlaciones entre varios factores, y compararlo con el historial de actividad de autenticación del usuario. Estas correlaciones son distintas combinaciones entre dispositivo, ubicación y franja horaria.

TrustedX Adaptive Authentication analiza el contexto en el que tiene lugar la autenticación y evalúa el riesgo de que se trate de un intento de suplantación de identidad.

Este análisis puede llevarse a cabo sin modificar la experiencia habitual del usuario y permite enriquecer cualquier proceso de autenticación en el que intervenga un nombre de usuario y una contraseña. Por lo tanto, es especialmente útil en entornos donde no sea posible usar mecanismos más fuertes, por ejemplo, por cuestiones de usabilidad (como suele suceder en entornos de gran consumo) o por el coste de despliegue de mecanismos más fuertes (como OTPs hardware).

Por lo tanto, el análisis del contexto de autenticación detecta anomalías en los procesos de autenticación, aumenta el nivel de seguridad que proporcionan las contraseñas por sí mismas, disminuye el riesgo de suplantación de identidad y aporta un grado mayor de confianza en la protección de los recursos.

El sistema almacena información detallada de todos los factores del contexto de los procesos de autenticación. Además, cuando se detecta una situación anómala, el sistema genera un evento que queda registrado como elemento de auditoría y que, además, se puede traducir en una alarma, o en la activación de algún factor de autenticación adicional que ayude a ratificar que el usuario es el propietario de las credenciales.