Autenticación segura por capas

Una defensa efectiva contra el phishing y el pharming

El mecanismo de autenticación basado en usuario y contraseña es el más usado en la actualidad. Históricamente, las ventajas de usabilidad que disfruta el usuario con un factor del tipo "algo que se sabe" han compensado el bajo nivel de seguridad que proporcionan las contraseñas. Obviamente, este mecanismo sólo se usa en escenarios y transacciones de riesgo bajo, pero, en general, y la práctica lo demuestra, es la puerta de acceso a la mayor parte de la "vida digital" cotidiana del usuario.

Existen múltiples ataques cuyo objetivo es el robo de una identidad digital protegida por un nombre de usuario y una contraseña. Y entre ellos, por su notoriedad y efectividad, destacan el *phishing* y su forma más sofisticada, el *pharming*. Básicamente, en un ataque de *phishing* se engaña al usuario haciéndole creer que está conectado a la página Web de su auténtico proveedor de servicio (su banco, la Administración, su aplicación de correo electrónico, una red social, etc.) para que introduzca su nombre de usuario y su contraseña en un proceso de autenticación que imita al del sitio Web original. De esta forma, el atacante recolecta nombres de usuario y contraseñas para utilizarlas de forma fraudulenta y suplantar al usuario legítimo.

El consorcio *Anti-Phishing Working Group* (APWG) difunde periódicamente estadísticas de ataques de *phishing* a nivel global. En el primer semestre de 2012[1] localizó 93.462 ataques, todos ellos concentrados en 486 objetivos, entre los que se encuentran bancos, sitios web de comercio electrónico, sitios web gubernamentales (sobre todo relacionados con Economía y Hacienda), sitios web de juegos en línea y, cada vez más, redes sociales, ISP y pro*veedore*s de correo electrónico.

[1] *R. Rasmussen, G. Aaron, "Global Phishing Survey: Trends and Domain Name Use in 1H2012", Octubre 2012.*

La cuestión es ¿cómo se puede mejorar la seguridad mientras se mantiene la usabilidad que proporciona la combinación de nombre de usuario y contraseña? ¿Y cuando se utiliza una credencial de otro dominio para acceder a un servicio, como ocurre cada vez más con el uso de cuentas de redes sociales, proveedores de Internet y de correo? La respuesta no siempre está en sustituir el mecanismo de autenticación más popular por otro más seguro, sino en introducir una estrategia de seguridad por capas (*layered security*) y añadir líneas de defensa a la autenticación (*defense in depth*).

La nueva solución de autenticación adaptativa de Safelayer implementa una estrategia de seguridad por capas a partir de una primera línea de autenticación, basada en nombre de usuario y contraseña. La protección ante ataques de *phishing* y *pharming* ilustra su funcionamiento, aunque la cobertura a otros tipos de ataques también está incluida: *offline cracking*, *online guessing*, *social engineering*, *eavesdropping*, etc.

Autenticación del sitio Web

El *phishing* tiene una dimensión psicológica en la medida en que los atacantes aprovechan limitaciones en el conocimiento técnico o descuidos en las buenas prácticas de seguridad para engañar a los usuarios. Las medidas contra este tipo de ataques, basados en ingeniería social, tienen una componente de prevención orientado a advertir al usuario medio de que algo no va bien durante su proceso de autenticación, que complementan a las medidas de prevención de robo de contraseñase impedir su uso fraudulento en los supuestos de robo.

Los ataques de *phishing* suelen iniciarse cuando el usuario hace clic en un enlace de un correo electrónico o una página Web que le lleva a un sitio falso. En general, a cualquier usuario no especialmente concienciado por la seguridad le resulta difícil detectar que están intentando engañarle para que revele su credencial. Por este motivo, es conveniente disponer de mecanismos de autenticación del sitio Web, con los que el usuario pueda reconocer fácilmente que el sitio al que se ha conectado es el legítimo. Y si este método de autenticación funcionara de forma evidente para el usuario medio, el robo de la credencial se evitaría en la mayoría de ocasiones.

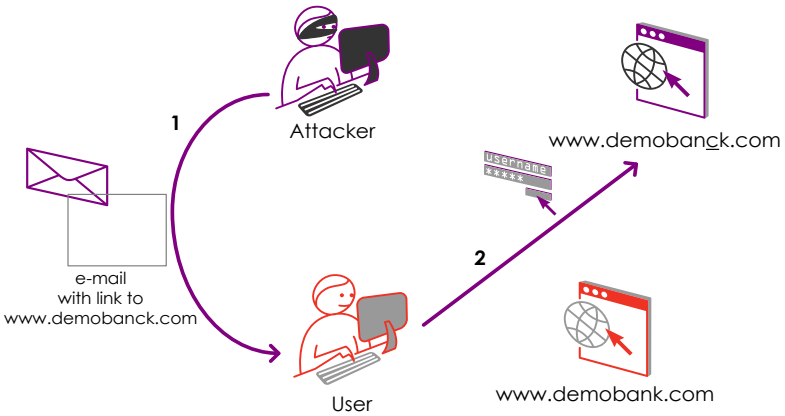

Figura: Proceso de un ataque de phishing

El método de autenticación en servidores web más utilizado se basa en el protocolo SSL/TLS. El navegador indica que un sitio web está autenticado mediante una imagen de un candado en la barra de navegación, de forma que el usuario puede confiar en el

sitio y enviar datos sensibles. No obstante, determinados estudios de usabilidad confirman que este método no es suficiente. Por ejemplo, *U.S. Department of Homeland Security, Science and Technology Directorate* (DHS S&T)[2]constata que la identificación visual de la imagen de un candado no es suficientemente efectiva para indicar al usuario que el sitio web no es fiable.

En el artículo *"Why Phishing Works"*[3] se estimó que el 23% de los usuarios no hace caso de las señales de advertencia de los navegadores en la barra de direcciones o la barra de estado, lo cual conduce a decisiones de seguridad erróneas en un 40% de las ocasiones. Las técnicas de engaño visuales son efectivas incluso para los usuarios más avanzados. Los resultados de este estudio revelan que los indicadores de seguridad estándares no son suficientemente efectivos para la mayoría de los usuarios, y concluye que son necesarias medidas adicionales.

En este sentido, Safelayer proporciona una solución en la que los usuarios pueden seleccionar una imagen personal para que se muestre en el formulario de entrada de las credenciales. La protección frente al *phishing* se deriva de que la imagen personalizada es diferente para cada dispositivo (es decir, para cada navegador dentro una cuenta de un sistema operativo). De este modo, aunque un sitio Web falso pueda replicar exactamente el formulario legítimo de entrada de las credenciales, no podrá replicar la imagen que espera ver el usuario, puesto que esta imagen es distinta para cada uno de ellos (y en general, para cada dispositivo que utilice).

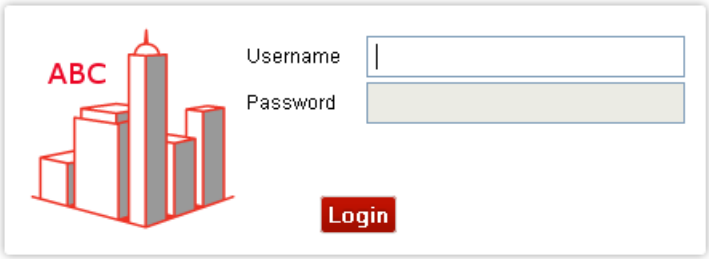

Figura: Imagen personalizada que se presenta en el formulario de introducción de credenciales. La ausencia de esta imagen habitual alerta al usuario de la suplantación del sitio.

En cuanto a la experiencia de uso que proporciona la solución basada en una imagen personalizada, es muy simple: si el usuario no ve la imagen que espera y a la que se ha habituado, abandona el impulso de introducir su credencial y, por tanto, habrá abortado el ataque de *phishing*.

Identificación del dispositivo

La solución descrita en el apartado anterior permite asociar una imagen personal a cada dispositivo. Para ello, el sitio Web que solicite la autenticación de los usuarios deberá identificar el dispositivo utilizado por cada uno de los usuarios para saber qué imagen debe mostrar.

[2] *A. Emigh, "Online Identity Theft: Phishing Technology, Chokepoints and Countermeasures (rev. 1.3)", Octubre 2005.*
[3] *R. Dhamija, J.D. Tygar, M. Hearst, "Why Phishing Works", Conference on Human Factors in Computing Systems, Abril 2006.*

Además, las ventajas de poder identificar el dispositivo también se extienden a la mejora del servicio de autenticación. En caso de que un impostor consiga engañar a un usuario y robar su credencial, intentará usarla desde un dispositivo distinto al que el usuario legítimo utiliza habitualmente, cosa que el servicio de autenticación podrá detectar, permitiéndole lanzar una alarma y reaccionar en consecuencia.

Una forma de identificación de dispositivos es mediante el uso de cookies y/o el análisis de un conjunto de características de éste. Según el *U.S. Federal Financial Institutions Examination Council (FFIEC)*[4] se distinguen mecanismos de identificación simples y complejos:

- Identificación de dispositivo "simple", en la que se utiliza una *cookie* estática y/o una dirección IP para identificar el dispositivo.
- Identificación de dispositivo "compleja", en la que se utilizan *cookies* de un solo uso (*one-time cookies*) y se crea una huella digital (*fingerprint*) del dispositivo en la que se incluyen características de éste como información de su configuración, dirección IP, geolocalización, etc.

FFIEC apunta que, si bien no existe ningún mecanismo de autenticación completamente fiable, la identificación de dispositivo compleja es más segura y preferible que la simple.

El beneficio clave de la identificación de dispositivo "compleja" es la relación entre la seguridad, el coste y el nivel de usabilidad que ofrece. En la siguiente tabla se pueden apreciar los niveles de disminución de riesgo vs los costes de usabilidad, económicos y de implementación en relación con otros mecanismos.

	Coste			Disminución de riesgo			
Capa	**De usabilidad**	**Económico**	**De implementación**	**De incidentes**	**Pérdidas financieras**	**Reputación dañada**	**Exposición Legal**
Plug-in seguro de navegador	Bajo - Moderado	Bajo - Moderado	Moderado - Alto	Alta	Alta	Alta	Moderada - Alta
Autenticación compleja de dispositivo	Bajo - Moderado	Bajo - Moderado	Moderado - Alto	Alta	Alta	Alta	Moderada - Alta
Imagen - Preguntas personalizadas	Bajo	Moderado	Bajo - Moderado	Baja - Moderada	Baja - Moderada	Baja - Moderada	Baja - Moderada
Contraseña fuerte	Bajo - Moderado	Bajo	Bajo - Moderado	Moderada	Moderada	Moderada - Alta	Alta
Token	Alto	Moderado - Alto	Alto	Moderada	Moderada	Moderada	Moderada

Figura: Tabla relación coste vs mitigación de riesgo de diferentes mecanismos de seguridad. (fuente: American Bankers Association).

La solución de Safelayer incluye una gestión basada en "identificadores complejos de dispositivo" en la que se utilizan *one-time cookies* y *fingerprints* a partir de múltiples parámetros del dispositivo. Los *fingerprints* identifican el contexto del dispositivo (CDI) incluyendo datos de configuración del sistema operativo y del navegador (versión actual mayor y menor, parches, fuentes, *plug-ins* instalados, etc.), localización geográfica y zona horaria.

La solución permite que el usuario registre explícitamente uno o más dispositivos como propios y de confianza, esto es, como un factor de autenticación del tipo "algo que se tiene". Con este registro, el usuario establece que dicho dispositivo permanece siempre bajo su posesión y control y, por tanto, que su uso proporciona garantías adicionales sobre su identidad. En consecuencia, se puede atribuir menor riesgo de suplantación a

[4] *"Supplement to Authentication in an Internet Banking Environment", Junio 2011.*

los accesos que realiza con dicho dispositivo que a los que realiza con otros dispositivos que no haya registrado.

Protocolo de doble *cookie* de un solo uso

Tal y como se ha visto anteriormente, las *cookies* pueden usarse para identificar a un dispositivo con el fin de mostrar la imagen personalizada por el usuario. En este caso, una *cookie* sería suficiente para mitigar la amenaza de un ataque de *phishing* simple, ya que el navegador nunca entregaría la *cookie* a un dominio diferente al del servidor legítimo, pero no aporta protección suficiente contra ataques de *phishing* avanzados, esto es, en un ataque de *pharming.*

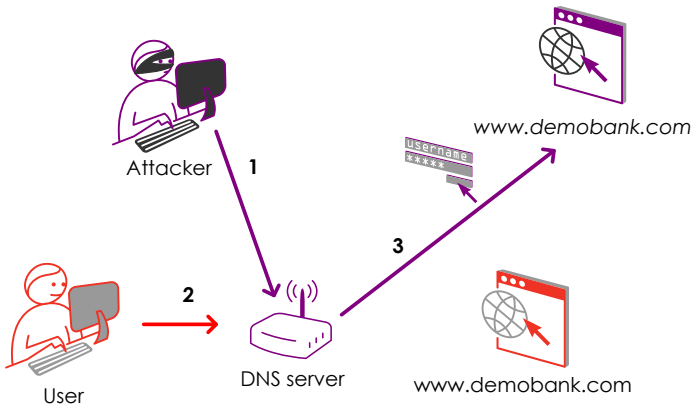

Figura: En el caso de un ataque de pharming, el atacante consigue hacer creer al navegador que el servidor fraudulento pertenece al mismo dominio que la cookie y, de esta forma robar de forma remota las cookies del navegador. En la figura se muestra cómo el atacante desvía al usuario a un www.demobank.com fraudulento suplantando previamente el sistema de nombres DNS.

Para combatir los ataques de *pharming*, la solución de Safelayer incorpora una capa de seguridad adicional mediante un protocolo que hemos denominado *one-time double-cookie protocol*, que se apoya en el uso de una combinación de dos *cookies* de un solo uso. Estas cookies tienen las siguientes características: están marcadas como *secure*, es decir, sólo se transmiten por SSL; están marcadas como *http-only* para que no puedan capturarse desde JavaScript y así mitigar ataques de *cross-site scripting*; tienen fecha de caducidad; están asociadas al dominio de la aplicación cliente, y su contenido es un valor aleatorio, es decir, ninguna de ellas contiene información acerca del usuario o el dispositivo, ni su contenido se genera a partir de variables del usuario o del dispositivo. Inicialmente, se generan y envían la primera vez que el usuario se autentica.

Mientras que la primera *cookie* (*Hello cookie*) se liga al nombre del dominio del servidor legítimo y sigue siendo atacable con técnicas de *pharming*, la segunda *cookie* (*ID cookie*) se liga a un *path* aleatorio que sólo es conocido por el servidor legítimo que la generó. De esta forma, para identificar al dispositivo, el servidor espera recibir dos *cookies* según el protocolo siguiente: en primer lugar recibirá la *Hello cookie*. El servidor utilizará esta *cookie* para hacer una identificación inicial del dispositivo y redireccionarlo a una página con el *path* exclusivo al que está ligada la *IDcookie*, que sólo conoce el servidor legítimo. Si el navegador finaliza el protocolo y envía la *ID cookie*, el servidor será capaz de completar la identificación del dispositivo y, por ejemplo, podrá mostrar la imagen personalizada. De esta forma, se habrá conseguido llevar a cabo un proceso de autenticación mutua entre dispositivo y servidor.

Para minimizar la posibilidad de que las cookies puedan ser utilizadas de forma fraudulenta si se llegan a capturar, el valor aleatorio contenido en las cookies se renueva cada vez que se obtiene la imagen personalizada (de forma previa a la autenticación) y cada vez que el usuario se autentica con éxito. El registro de dispositivos por parte del usuario no implica ninguna modificación en el protocolo de intercambio de cookies ni en su contenido.

En resumen, gracias al protocolo *one-time double-cookie*, ningún servidor fraudulento será capaz de provocar el envío de la segunda *cookie* porque no conoce el *path* exclusivo al que está asociada y quedará abortado el ataque de *pharming*. Con la introducción de esta nueva capa de seguridad, la solución mejora las expectativas de la FFIEC, en cuanto a la identificación compleja del dispositivo, y de la mayoría de soluciones existentes en la actualidad basadas en una *one-time cookie.*

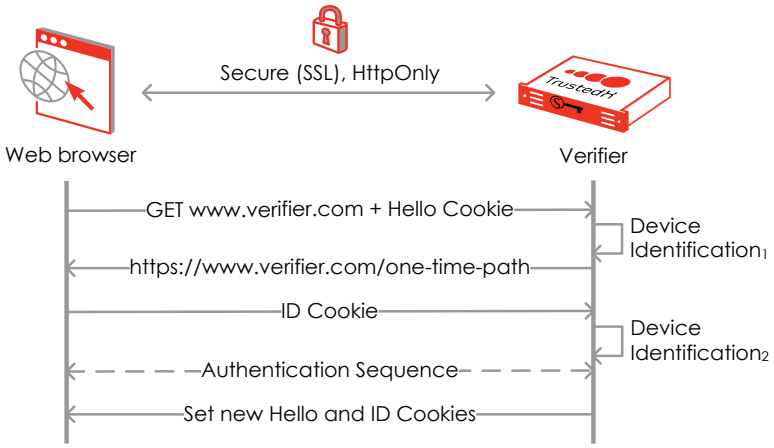

Figura: Protocolo de doble cookie de un solo uso que implementa TrustedX

Autenticación adaptativa de Safelayer

La solución de autenticación adaptativa de Safelayer maximiza el nivel de seguridad de la autenticación con una aproximación por capas (*Layered Security*), a la vez que minimiza el coste de implementación y despliegue, así como, muy importante, el de usabilidad por parte de los usuarios.

La solución aumenta la seguridad de la primera línea de autenticación, basada en nombre de usuario y contraseña, con la introducción de medidas adicionales como la presentación de una imagen personalizada y la identificación compleja de dispositivo mediante el protocolo *one-time double-cookie.* Por otra parte, incorpora un motor de análisis del contexto del usuario que permite evaluar el riesgo de suplantación a partir de la correlación de parámetros de dispositivo, de localización, cronológicos y otros. En base al resultado del análisis, cuenta con la posibilidad de ejecutar una segunda línea de autenticación, por ejemplo, un código único en un mensaje SMS o *e-mail*, un código único generado en un dispositivo OTP o en una aplicación para el móvil, o en general cualquier mecanismo que se pueda integrar al sistema.

El análisis de contexto puede complementarse con un sistema biométrico que reconoce la dinámica de tecleo del usuario. Esta línea de defensa se integra transparentemente en el formulario de entrada del nombre de usuario y contraseña (o cualquier campo equivalente y adicional) de forma que el motor de análisis puede determinar si el

usuario que ha tecleado la credencial es el legítimo, comparando el patrón de tecleo detectado con el que tiene registrado. Con este mecanismo se puede detectar si el usuario legítimo, ya sea de forma voluntaria o no, ha cedido su credencial a otro usuario, mitigando también los ataques que se basan en la ingeniería social.

Mediante un sistema basado en políticas, la organización puede ajustar las capas de seguridad (primera línea, análisis de riesgo del contexto y segunda línea) a los escenarios que mejor se adapten a sus requisitos de seguridad, de coste y a sus usuarios.

Estas capas de seguridad en autenticación deben complementarse con otras, especialmente las relacionadas con i) la educación, vigilancia y relación con los usuarios, y ii) el análisis de inteligencia. Mientras que la primera conciencia y compromete al usuario en buenas prácticas de seguridad, la segunda refuerza la toma de decisiones en la autorización de accesos y transacciones de alto riesgo. En esta línea, la información capturada y generada en la fase de autenticación es de gran valor para la inteligencia de negocio. En definitiva, siempre es mejor optimizar la usabilidad y comodidad en el lado del usuario, y la seguridad y coste en el lado *back-end*.

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.