LIBRO BLANCO | DICIEMBRE DE 2014

Solucionando el mayor problema de seguridad en la entrega de aplicaciones web

Gestión del pirateo de sesiones con CA Single Sign-On Enhanced Session Assurance with DeviceDNA™

Martin Yam
Equipo de Gestión de Seguridad de CA

ca technologies

Resumen ejecutivo

Reto

Desde los comienzos de la entrega de aplicaciones web, los piratas informáticos han aprovechado la oportunidad para irrumpir en mitad de una transacción y suplantar la identidad del usuario legítimo. Ya que las credenciales necesarias para perpetrar este fraude son válidas y se espera que el usuario real sea responsable de ellas, este tipo de suplantación de identidad es difícil o incluso imposible de detectar y detener.

Oportunidad

La amenaza del pirateo de sesiones es un tema que genera cada vez más preocupación entre las empresas que cuentan con activos que requieren protección, pero que al mismo tiempo desean proporcionar a sus usuarios un acceso a estos activos sencillo pero seguro. Es uno de los problemas de seguridad más importantes a los que se enfrentan las empresas actualmente. Numerosos expertos importantes en el tema consideran el pirateo de sesiones como un riesgo de seguridad prácticamente permanente (consulte Wikipedia.org).

El Proyecto abierto de seguridad de aplicaciones web (OWASP, por sus siglas en inglés) hace hincapié en esta vulnerabilidad en la lista Top 10 de 2013[1]. Las dos categorías que se incluyen a continuación se refieren a casos específicos de fallos en la autenticación y pirateo de sesiones.

1. A2 (infracciones de autenticación y gestión de sesiones)
2. A3 (generación de scripts entre sitios [XSS])

Esto pone en evidencia la alta visibilidad del problema y otorga un gran valor a cualquier remedio que ayude a abordarlo.

Ventajas

CA Technologies ha desarrollado una solución para este problema de seguridad que va más allá de las soluciones listas para usar (COTS, por sus siglas en inglés) y las soluciones de gestión del acceso a la Web (WAM, por sus siglas en inglés) de cosecha propia. Este método consiste en vincular las credenciales válidas del usuario y la cookie de la sesión a la identificación del dispositivo que utiliza el usuario para iniciar sesión originalmente. La comprobación y la validación periódicas de esta combinación de las credenciales y el dispositivo durante una sesión de transacciones permite garantizar que el usuario real es quien desarrolla toda la transacción y que no se ha pirateado la sesión.

Sección 1

La importancia de la autenticación continua

El pirateo de sesiones, también denominado "pirateo de cookies", no es una amenaza reciente; de hecho, ha evolucionado hasta considerarse un riesgo de seguridad prácticamente permanente desde que HTTP 1.1 pasó a ser el protocolo estándar. Un informe elaborado recientemente por Forrester Research trata sobre la autenticación continua, hecho que, desde nuestro punto de vista, identifica la amenaza que supone el pirateo de sesiones. El punto 4 del informe de Forrester Research, "OUR PREDICTIONS FOR IAM IN 2014"[2] dice lo siguiente:

> ***"La autenticación continua protegerá cada sesión de principio a fin.*** *El uso de direcciones IP, o ID de dispositivos y su reputación ya no es un método de protección suficiente frente a las amenazas. Esto se debe a que estos parámetros afectan principalmente al primer paso de las interacciones de los usuarios, es decir, a la autenticación inicial. Una vez que el usuario ha iniciado sesión, la protección que ofrecen es mínima. Pase a la autenticación continua, que consiste en observar el comportamiento del usuario (principalmente en la Web durante la primera fase de observación y en otros canales durante las fases posteriores) para determinar si desarrolla una conducta disciplinada al navegar por el sitio. Si se detecta cualquier motivo de alarma (por ejemplo, que el agente del usuario esté extrayendo datos de sitios a gran velocidad o que se esté produciendo un ataque o una extracción de datos), la solución puede avisar a los administradores e incluso, de forma opcional, cerrar la sesión.*
>
> ***Medidas que puede tomar.*** *Para protegerse frente a sesiones sospechosas, deberá establecer una línea de referencia del buen comportamiento. Deberá solicitar a su distribuidor de soluciones de autenticación en función del riesgo (RBA, por sus siglas en inglés) que compruebe si es posible establecer una línea de referencia de la actividad del usuario antes de que se inicien las operaciones habituales, ya que obtener esta información de cualquier otra forma es prácticamente imposible".*

CA Technologies ofrece la tecnología Enhanced Session Assurance with DeviceDNA para proporcionar autenticación continua. Esta función está disponible de serie para los usuarios de CA Single Sign-On r12.52. A través de otra función de CA Single Sign-On denominada "Session Linking" ("vinculador de sesión"), esta capacidad también puede ampliarse para proteger las aplicaciones que usan sus propias cookies de sesión, como Tivoli Access Manager, Oracle Access Manager o muchas otras soluciones de cosecha propia. Es importante destacar que para ello no es necesario llevar a cabo ninguna modificación en dichas aplicaciones.

Enhanced Session Assurance with DeviceDNA funciona aprovechando los componentes de las soluciones de CA existentes. Además, utiliza la capacidad incluida en el sistema CA Risk Authentication para identificar y recopilar las características técnicas del dispositivo del usuario legítimo a partir de la secuencia de inicio de sesión original y cotejarlas periódicamente con las del dispositivo real que esté utilizando la cookie de la sesión durante la sesión del usuario. El período de comprobación del dispositivo puede configurarse para mejorar el rendimiento y hacer que las comprobaciones tengan lugar en las partes más importantes de la sesión.

Cómo ocurre el problema

El objetivo de los piratas informáticos es aprovechar el procedimiento más sencillo para acceder ilícitamente a un sistema. Gracias a la implementación cada vez más extendida de otras tecnologías de autenticación, resulta más difícil piratear las credenciales de inicio de sesión de un usuario, por lo que los piratas informáticos están investigando métodos innovadores y originales para acceder a los flujos de transacciones válidos y ya autenticados. Se espera que esta nueva táctica siga creciendo a un ritmo aún más rápido en el futuro.

Algunas empresas optan por aplicar credenciales más seguras para intentar evitar que los piratas informáticos consigan las cookies de sesión. Las credenciales de dos factores que proporciona CA Strong Authentication pueden contribuir a crear un sistema de seguridad inicial, pero mediante el uso de credenciales de un único factor, como un nombre de usuario y una contraseña de Active Directory (AD), el reto reside en la seguridad que ofrece la aplicación una vez que el pirata informático ha logrado acceder a la sesión. El uso de información basada en red puede resultar útil, pero los dispositivos que trabajan con varias redes pueden camuflar u ocultar las direcciones IP fácilmente.

Enhanced Session Assurance with DeviceDNA y los sistemas de autenticación continua de CA Technologies suponen un avance significativo en cuanto a la prevención de la reproducción de sesiones pirateadas.

Gracias al uso de la tecnología DeviceDNA pendiente de patente, disponible en CA Risk Authentication, CA Single Sign-On logra identificar el cliente y determinar si el dispositivo que ha accedido a la sesión ha cambiado en mitad de esta.

CA Single Sign-On realizará comprobaciones regularmente, en periodos que pueden configurarse, para verificar que el dispositivo cliente actual coincide con el dispositivo desde el que se inició sesión originalmente. Si se detecta alguna discrepancia, hay muchas probabilidades de que un atacante haya pirateado la sesión. En este caso, la aplicación puede solicitar al usuario que vuelva a identificarse mediante unas credenciales secundarias o expulsarle de la sesión y mostrarle un mensaje en el que se le indica que debe volver a iniciarla. Esta función puede activarse en las aplicaciones que desee individualmente. Cada aplicación puede tener un periodo de comprobación distinto según el valor del activo al que protege o permite acceso.

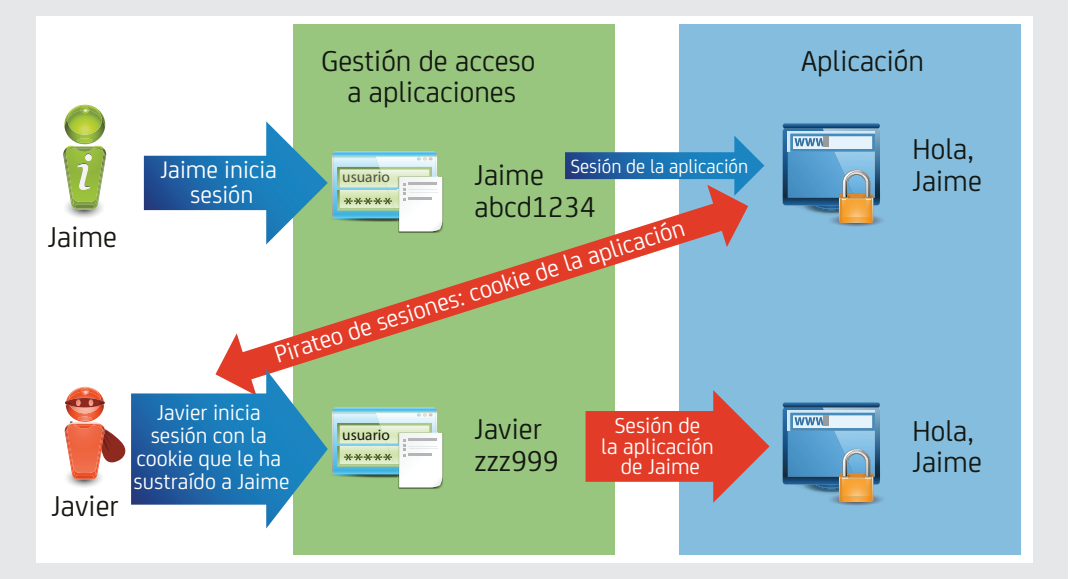
En el gráfico que aparece a continuación se describe un proceso de pirateo de sesión y la amenaza que esto supone para la aplicación empresarial.

Paso 1: Jaime, el usuario legítimo, inicia sesión y se autentifica en la aplicación.

Paso 2: Javier, el pirata informático, sustrae las credenciales de la cookie de la sesión de Jaime.

Paso 3: Javier inicia sesión utilizando las credenciales de cookie de la sesión de Jaime; la aplicación considera que se trata de Jaime, lo reconoce como usuario legítimo y le proporciona el mismo acceso.

Ilustración A.



Sección 2

Ampliación de la comprobación continua de la sesión a la aplicación

CA Access Gateway ofrece otra función que permite ampliar la seguridad de la sesión de CA Single Sign-On hasta la sesión de la aplicación. La función de vinculador de sesión está diseñada para examinar las solicitudes de entrada y validar que las cookies de sesión de las aplicaciones solo se utilizan en combinación con la sesión de CA Single Sign-On para la que se han creado. Si esta función detecta que un usuario presenta una cookie de aplicación de un usuario distinto y una sesión de CA Single Sign-On propia (para tratar de burlar las comprobaciones de seguridad de la sesión), se le expulsará de la sesión. Un usuario puede usar esta función de vinculador de sesión en combinación con Enhanced Session Assurance with DeviceDNA para proteger las cookies de una aplicación o incluso los tokens correspondientes a otras soluciones de gestión del acceso a la Web que no pertenezcan a CA Single Sign-On.

Sección 3

Conclusión

El pirateo de sesiones no es un riesgo que haya surgido recientemente; de hecho, existe desde la aparición del protocolo HTTP 1.1. Sin embargo, la notoriedad de esta amenaza ha aumentado en los últimos años y las organizaciones son conscientes de la necesidad de tomar medidas para combatirla.

CA Technologies ha desarrollado una solución para enfrentarse al pirateo de sesiones que consiste en comparar las credenciales válidas de un usuario y la cookie de la sesión interna con la identificación del dispositivo que utiliza el usuario para iniciar sesión originalmente. Enhanced Session Assurance with DeviceDNA proporciona un sistema de autenticación continua y está disponible de serie para los usuarios de CA Single Sign-On r12.52. Se trata del único producto de este tipo que puede ayudar a evitar el pirateo de sesiones.

Sección 4

Definiciones

¿Qué es CA Single Sign-On?

CA Single Sign-On es un conjunto de soluciones de gestión de acceso flexibles y de alta escalabilidad que proporcionan un inicio de sesión único seguro, la autorización basada en políticas, así como la auditoría y la administración de aplicaciones en la nube y en la Web. CA Federation admite la federación de identidades basada en estándares, con lo que permite que los usuarios accedan de forma segura a las aplicaciones de los distintos dominios. Resulta útil conseguir que su presencia en línea sea segura, esté disponible y tenga fácil acceso, sin que los límites organizativos dificulten el camino. CA Access Gateway facilita una puerta de enlace de proxy que proporciona un modelo de implementación opcional en el conjunto de soluciones de inicio de sesión único seguro y una gestión de accesos flexible. Esto permite desarrollar negocios en línea de forma segura y habilita el inicio de sesión único.

¿Qué es CA Advanced Authentication?

CA Advanced Authentication es una solución flexible y escalable que incorpora métodos de autenticación basados en riesgos como la identificación y la geolocalización de dispositivos y la actividad del usuario, así como una amplia variedad de credenciales de autenticación sólidas y de varios factores. Esta solución permite a la organización crear el proceso de autenticación adecuado para cada aplicación o transacción. Puede entregarse como software in situ o como un servicio en la nube, así como proteger el acceso a la aplicación desde una amplia gama de terminales, incluidos todos los dispositivos móviles comunes. Esta completa solución permite a las organizaciones aplicar de forma rentable el método apropiado de autenticación sólida en todos los entornos sin sobrecargar a los usuarios finales.

CA Strong Authentication es un servidor de autenticación versátil que le permite implementar y aplicar una amplia variedad de métodos de autenticación sólidos de forma eficaz y centralizada. Permite la interacción en línea segura con sus empleados, clientes y ciudadanos, ya que ofrece una autenticación sólida de varios factores tanto para aplicaciones internas como en la nube. Incluye aplicaciones de autenticación para dispositivos móviles y SDK, así como numerosas formas de autenticación Out-of-band.

CA Risk Authentication ofrece a su organización un sistema de autenticación de varios factores que puede detectar y bloquear los fraudes en tiempo real sin necesidad de interactuar con el usuario. Se integra con cualquier aplicación en línea, incluidos sitios web, portales y VPN, y analiza el riesgo de que se produzcan intentos de acceso y transacciones en línea. Este método de autenticación de varios factores, que el usuario final no percibe en absoluto, utiliza factores contextuales como el ID del dispositivo, la geolocalización, la dirección IP y la información de la actividad de usuario, para calcular el riesgo y recomendar la acción adecuada.

DeviceDNA identifica los dispositivos que acceden a sus aplicaciones. Proporciona un resumen de información sobre la naturaleza del dispositivo, como el tipo de dispositivo y el ID de dispositivo exclusivo, para poder evaluar el nivel de riesgo.

Sección 5

Más información

La función de vinculador de sesión se analiza más detalladamente en un libro blanco de CA Technologies asociado a este y llamado “Vinculador de sesión y seguridad de sesión”.

Sección 6

Acerca del autor

Martin Yam es consultor de estrategias de CA Technologies. Antes de empezar a trabajar en CA Technologies, Yam fue Vicepresidente de Ventas Internacionales en Arcot Systems, Inc. Yam también ha ocupado cargos de directivo y relacionados con la gestión de ventas en Oracle, Informix, Accrue Software, ParcPlace Systems y NeXT.

Comuníquese con CA Technologies en ca.com/es

CA Technologies (NASDAQ: CA) crea software que impulsa la transformación de las empresas y les permite aprovechar las oportunidades de la economía de aplicaciones. El software se encuentra en el corazón de cada empresa, sea cual sea su sector. Desde la planificación hasta la gestión y la seguridad, pasando por el desarrollo, CA trabaja con empresas de todo el mundo para cambiar la forma en que vivimos, realizamos transacciones y nos comunicamos, ya sea a través de la nube pública, la nube privada, plataformas móviles, entornos de mainframe o entornos distribuidos. Para obtener más información, visite **ca.com/es**.

1 La URL completa es https://www.owasp.org/index.php/Top_10_2013-Top_10

2 "Predictions 2014: Identity And Access Management, Employee And Customer IAM Head For The Cloud". Forrester Research, Inc., 7 de enero de 2014.

CS87229_0914