DOCUMENTO OFICIAL | DICIEMBRE DE 2014

Punto final para la brecha de seguridad más grande en la entrega de aplicaciones web

Abordar el robo de sesión con CA Single Sign-On Enhanced Session Assurance with DeviceDNA™

Martin Yam
Equipo de CA Security Management

ca technologies

Resumen ejecutivo

Desafío

Desde el comienzo de la entrega de aplicaciones web, ha habido oportunidades para que los estafadores intervengan en una transacción y se hagan pasar por el usuario legítimo. Dado que las credenciales utilizadas para este tipo de fraude son válidas y "se espera que las controle el usuario real", este tipo de suplantación de identidad ha sido difícil, o más bien imposible, de detectar y detener.

Oportunidad

Las empresas con activos que proteger están cada vez preocupadas por la amenaza de "robo de sesión", mientras que a la misma vez necesitan proporcionar un acceso fácil pero seguro a los usuarios. Es uno de los principales problemas que enfrentan las empresas hoy en día. Muchos expertos de primera línea identifican el "robo de sesión" como un riesgo de seguridad prácticamente permanente (consulte Wikipedia.org).

El Proyecto abierto de seguridad de aplicaciones web (OWASP, por su sigla en inglés) destaca esta vulnerabilidad en su lista de los Primeros 10 de 2013[1]. Las dos categorías que se enumeran abajo son casos específicos de mala autenticación y robo de sesión.

1. A2 – Autenticación rota y Administración de sesión
2. A3 – Secuencias de comandos entre sitios (XSS)

Esto destaca el alto perfil de este problema y hace que la solución que ayude a abordarlo sea mucho más valiosa.

Beneficios

CA Technologies ha desarrollado una solución a este problema de seguridad que va más allá de todas las soluciones comerciales disponibles listas para su uso (COTS) y la Administración de accesos web (WAM) casera mediante la vinculación de las credenciales válidas del usuario, y la cookie de sesión a la huella digital del dispositivo que fue utilizada para la sesión del usuario original. La verificación periódica de esta combinación de credencial y dispositivo durante una sesión de transacción y su validación pueden garantizar que el usuario real continúe su transacción y que su sesión no se intercepte.

Sección 1

La importancia de la "Autenticación continua"

El robo de sesión, también conocido como robo de cookie, no es una amenaza nueva, ha evolucionado en un riesgo de seguridad casi permanente desde que HPPT 1.1 se convirtió en un estándar. Un reporte de Forrester Research reciente analiza 'la autenticación' continua que, en nuestra opinión, reconoce la amenaza que representa el robo de sesión. La número cuatro en “OUR PREDICTIONS FOR IAM IN 2014”[2] en Forrester Research es:

La autenticación continua protegerá las sesiones de inicio a fin. *El uso de direcciones IP, de identificaciones del dispositivo y su reputación ya no son suficientes para proteger contra amenazas porque estos parámetros afectan principalmente solamente al primer paso en las interacciones de usuarios, autenticación de la puerta delantera. Una vez que el usuario inicia sesión, ofrecen poca protección. Ingrese la autenticación continua: observar el comportamiento del usuario (en particular en el canal web en la primera fase y en otros canales en fases siguientes) para determinar si el usuario está navegando el sitio de manera ordenada. Si hay razón de alarma, el agente del usuario raspando el sitio a alta velocidad o hay una sospecha de un ataque o exfiltración de datos, la solución puede alertar a los administradores y, opcionalmente, incluso finalizar la sesión.*

Lo que debe hacer. *A fin de protegerse contra sesiones sospechosas, debe establecer una buena referencia de conducta. Deberá preguntarle a su proveedor de solución de autenticación basada en riesgos (RBA, por su sigla en inglés) si puede establecer una referencia de actividad del usuario antes del inicio de las operaciones de rutina, ya que es casi imposible obtener esta información de otra manera.*

CA Technologies ofrece Enhanced Session Assurance with DeviceDNA para proporcionar 'autenticación continua' y está disponible de manera inmediata para los usuarios de CA Single Sign-On r12.52. A través de otra función de CA Single Sign-On llamada "Session Linking", esta capacidad también puede ampliarse para proteger las aplicaciones que utilizan sus propias cookies de sesión, como Tivoli Access Manager, Oracle Access Manager u otras soluciones caseras. Es importante destacar que se puede hacer esto sin modificaciones obligatorias para estas otras aplicaciones.

Enhanced Session Assurance with DeviceDNA aprovecha los componentes de solución de CA existentes. Utiliza la habilidad que ofrece CA Risk Authentication para identificar y recolectar características de equipo del dispositivo del usuario legítimo desde la secuencia de inicio de sesión y para comparar de manera periódica con el dispositivo real que está con la cookie de sesión durante la sesión del usuario. El tiempo entre los controles del dispositivo es configurable para mejorar el desempeño y para permitir que el control ocurra en partes de gran valor de la sesión.

Cómo ocurre el problema

Los hackers quieren explotar el camino más fácil para infiltrarse en un sistema. Con el aumento de la adopción de otras tecnologías de autenticación, el robo de credenciales es más difícil de modo que los estafadores buscan maneras nuevas y creativas de irrumpir en un flujo de transacción autenticado y válido. Se espera que esta explotación continúe creciendo a mayor velocidad en el futuro.

Se pueden utilizar credenciales más sólidas a medida que las empresas intentan evitar que un hacker robe una cookie de sesión. Las credenciales de dos factores entregadas como CA Strong Authentication pueden ayudar a construir la seguridad en la puerta de entrada, pero en el caso de credenciales de un único factor como usuario/contraseña Active Directory (AD), el desafío depende de cuan buena sea la seguridad de la aplicación LUEGO del robo de sesión. El uso de información basada en la red puede ser de ayuda, pero varios dispositivos de red pueden falsificar o esconder direcciones IP.

Enhanced Session Assurance with DeviceDNA/La autenticación continua de CA Technologies representa un paso crucial en el camino de la prevención de la repetición de robo de sesión.

Mediante el aprovechamiento de la tecnología DeviceDNA con patente en trámite y disponible en CA Risk Authentication, CA Single Sign-On puede identificar el cliente y determinar si el dispositivo de acceso ha cambiado durante la sesión.

De manera periódica y configurable, CA Single Sign-On vuelve a verificar que el dispositivo del cliente actual sea idéntico al dispositivo que originalmente ingresó para iniciar la sesión. Si no hay coincidencia, es muy probable que un atacante haya robado la sesión. En este caso, la aplicación puede solicitar que el usuario vuelva a autenticar con credenciales secundarias, o simplemente puede finalizar la sesión con un mensaje de reinicio de sesión. Esta función puede habilitarse de acuerdo con la aplicación. Diferentes aplicaciones tienen tasas de reverificación diferentes de acuerdo con el valor del activo que se accede o protege.

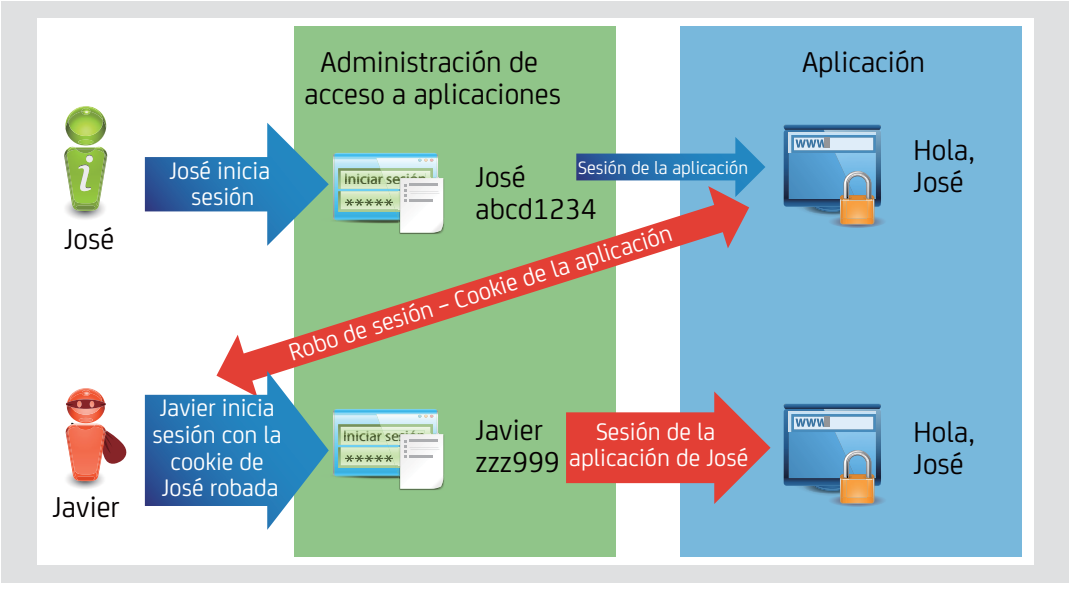
El siguiente gráfico describe la manera en que ocurre un robo de sesión y la amenaza que genera para la aplicación de la empresa.

Paso 1: Jaime, el usuario legítimo, inicia sesión y es autenticado para la aplicación.

Paso 2: José, el estafador, roba la credencial de cookie de la sesión de Jaime.

Paso 3: José ahora inicia sesión con la credencial de cookie de la sesión de Jaime; la aplicación piensa que es Jaime, sabe que él es un usuario legítimo y le otorga el mismo acceso.

Ilustración A.



Sección 2

Ampliar el aseguramiento de sesión continuo a la aplicación

CA Access Gateway ofrece otra función que puede ampliar esta seguridad para la sesión de CA Single Sign-On hasta la sesión de la aplicación también. La función Session Linker está diseñada para evaluar solicitudes entrantes para validar que las cookies de sesión de aplicaciones solamente se usen en conjunto con la sesión de CA Single Sign-On para la cual fueron creadas. Session Linker finaliza la sesión del usuario si detecta que un usuario presenta una cookie de aplicación de otro usuario, y su propia sesión de CA Single Sign-On (para intentar pasar por encima de los controles de aseguramiento de sesión). Es posible utilizar esta función Session Linking junto con Enhanced Session Assurance with DeviceDNA para proteger las cookies de aplicación o incluso los tokens de otras soluciones que no sean CA Single Sign-On Web Access Management (WAM).

Sección 3

Conclusión

El robo de sesión no es un riesgo de seguridad nuevo, existe desde HPPT 1.1. Sin embargo, su perfil ha aumentado recientemente y las organizaciones son conscientes de la necesidad de implementar medidas para combatirlo.

CA Technologies ha desarrollado una solución para abordar el robo de sesión que compara las credenciales válidas de un usuario final y la cookie de sesión interna con la huella digital del dispositivo que se utilizó para la sesión de usuario original. Enhanced Session Assurance with DeviceDNA proporciona "autenticación continua" y está disponible de manera inmediata para los usuarios de CA Single Sign-On r12.52, y es el único producto de su clase que puede ayudarlo a evitar el robo de sesión.

Sección 4

Definiciones

¿Qué es CA Single Sign-On?

Las soluciones de administración de acceso flexible CA Single Sign-On son soluciones de administración de acceso muy escalables y flexibles que proporcionan un inicio de sesión seguro, autorización basada en políticas, auditoría y administración para aplicaciones web y en la nube. CA Federation respalda que la federación de identidad basada en normas permita a los usuarios acceder de manera segura a aplicaciones entre dominios. Ayuda a hacer que su presencia en línea sea segura, disponible y accesible, sin límites institucionales que se interpongan. Además, CA Access Gateway entrega una puerta de enlace proxy de alto desempeño que proporciona un modelo implementación opcional en la familia de administración de acceso flexible y SSO seguro para habilitar de manera segura los negocios en línea y 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 de dispositivos, la geolocalización y las actividades del usuario, además de una amplia variedad de credenciales de autenticación sólidas, de múltiples factores. Esta solución puede permitir a la organización crear el proceso de autenticación apropiado para cada aplicación o transacción. Se puede entregar como software local o como servicio en la nube, y puede proteger el acceso a las aplicaciones desde una amplia gama de terminales, incluidos todos los dispositivos móviles populares. Esta solución integral puede habilitar a su organización a hacer cumplir de manera rentable el método apropiado de autenticación sólida en los diversos entornos sin poner la carga en los usuarios finales.

CA Strong Authentication es un servidor de autenticación versátil que le permite implementar y aplicar una amplia gama de métodos sólidos de autenticación de un modo eficiente y centralizado. Permite una interacción en línea segura con sus empleados, clientes y cuidados al ofrecer una autenticación sólida de múltiples factores para las aplicaciones internas y basadas en la nube. Incluye aplicaciones de autenticación móvil y SDK (kits de desarrollo de software), como así también varias formas de autenticación OOB (fuera de banda).

CA Risk Authentication ofrece a su organización una autenticación de factores múltiples que puede detectar y bloquear fraudes en tiempo real, sin ninguna interacción con el usuario. Se integra con cualquier aplicación en línea, incluidos sitios web/portales y VPN (redes privadas virtuales) para analizar el riesgo de transacciones e intentos de acceso en línea. Esta forma de autenticación de factores múltiples, que es invisible para el usuario final, utiliza factores contextuales como ID de dispositivo, ubicación geográfica, dirección IP e información de actividad del usuario, para calcular el riesgo y recomendar una medida adecuada.

DeviceDNA identifica los dispositivos que acceden a las aplicaciones. A fin de poder evaluar el nivel de riesgo se proporciona la información de resumen sobre la naturaleza del dispositivo como el tipo de dispositivo y la identificación de dispositivos únicos.

Sección 5

Para obtener más información

Se aborda con más detalle Session Linking en un documento oficial adjunto de CA Technologies llamado “Session Linking and Session Assurance”.

Sección 6

Acerca del autor

Martin Yam es asesor de estrategia de CA Technologies. Antes de ingresar en CA Technologies, Yam fue vicepresidente de ventas globales para Arcot Systems, Inc. Yam también prestó servicios de administración de ventas y ejecutivos en Oracle, Informix, Accrue Software, ParcPlace Systems y NeXT.

1 El URL completo 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.