DOCUMENTAÇÃO TÉCNICA | DEZEMBRO DE 2014

Fechando a maior lacuna de segurança na entrega de aplicativos web

Resolvendo o sequestro de sessão com o CA Single Sign-On Enhanced Session Assurance with DeviceDNA™

Martin Yam
Equipe de Gerenciamento de segurança da CA

ca technologies

Resumo executivo

Desafio

Desde o início da entrega de aplicativos web, tem havido uma oportunidade para os fraudadores interceptarem uma transação a fim de personificar o usuário legítimo. Como as credenciais usadas para essa fraude são válidas e "presumivelmente estão sob o controle do usuário", esse tipo de personificação tem sido difícil, se não impossível, de detectar e parar.

Oportunidade

A ameaça de "sequestro de sessão" é uma área de preocupação cada vez maior entre empresas com ativos para proteger e, ao mesmo tempo, fornecer acesso fácil, mas seguro, a seus usuários. Esse é um dos principais problemas de segurança enfrentados pelas empresas atualmente. Muitos especialistas líderes identificam o "sequestro de sessão" como um risco quase permanente de segurança (consulte a Wikipedia.org).

O Open Web Application Security Project (OWASP) destaca essa vulnerabilidade em sua lista das 10 maiores de 2013[1]. As duas categorias listadas abaixo são casos específicos de autenticação inadequada e sequestro de sessão.

1. A2 – Gerenciamento de autenticação e sessão desfeitas
2. A3 – XSS (Cross-Site Scripting - script entre sites)

Isso indica a alta visibilidade desse problema e torna uma solução que possa ajudar a resolvê-lo muito mais valiosa.

Benefícios

A CA Technologies desenvolveu uma solução para esse problema de segurança que atravessa todas as soluções de COTS (commercial off-the-shelf - comerciais prontas para uso) e WAM (Web Access Management - Gerenciamento de acesso à web) desenvolvidas internamente, ligando as credenciais válidas do usuário e o cookie de sessão à superfície do dispositivo que foi usado para o logon inicial do usuário. Verificar periodicamente essa combinação de credencial/dispositivo durante uma sessão de transação e validá-la pode garantir que o usuário atual está continuando sua transação e que sua sessão não foi sequestrada.

Seção 1

A importância da "autenticação contínua"

O sequestro de sessão, também conhecido como sequestro de cookie, não é uma ameaça recente, tendo evoluído para um risco de segurança quase permanente desde que o HTTP 1.1 se tornou um padrão. Um relatório recente da Forrester Research discutiu a 'autenticação contínua' que, da nossa perspectiva, reconhece a ameaça que o sequestro de sessão representa. O item número quatro de "OUR PREDICTIONS FOR IAM IN 2014"[2] da Forrester Research é:

A autenticação contínua protegerá as sessões do início ao fim. *O uso de endereços IP ou IDs de dispositivos e sua reputação não é mais suficiente para proteger-se contra ameaças porque esses parâmetros afetam principalmente apenas a primeira etapa das interações do usuário: autenticação na porta de entrada. Depois que o usuário está conectado, eles oferecem pouca proteção. Entra em cena a autenticação contínua: observar o comportamento do usuário (principalmente no canal web na primeira fase e em outros canais em fases posteriores) para determinar se o usuário está navegando pelo site de uma maneira ordenada. Se houver motivo para alarme (o agente do usuário está varrendo o site em altas velocidades ou há uma suspeita de um ataque ou de exfiltração de dados) a solução pode alertar os administradores e opcionalmente até terminar a sessão.*

O que você precisa fazer a respeito *Para proteger-se contra sessões suspeitas, você precisa estabelecer uma linha de base de bom comportamento. Você precisará pedir ao fornecedor da sua solução RBA (risk-based authentication - autenticação com base em riscos) para verificar se é possível estabelecer uma linha de base de atividades de usuários antes de as operações de rotina começarem, porque obter essas informações de outra maneira é quase impossível.*

A CA Technologies oferece Enhanced Session Assurance with DeviceDNA para fornecer "autenticação contínua", e ele está disponível "pronto para uso" para usuários do CA Single Sign-On r12.52. Através de outro recurso do CA Single Sign-On chamado "Vinculação de sessão", esse recurso também pode ser estendido para proteger os aplicativos que usam seus próprios cookies de sessão, como o Tivoli Access Manager, o Oracle Access Manager ou muitas soluções desenvolvidas localmente. É importante observar que isso pode ser feito sem nenhuma modificação nesses outros aplicativos.

O Enhanced Session Assurance with DeviceDNA aproveita os componentes de soluções existentes da CA. Ele usa a capacidade contida no CA Risk Authentication para identificar e coletar características da máquina do dispositivo do usuário legítimo de sua sequência de logon inicial e as compara periodicamente com o dispositivo real que está com o cookie de sessão durante a sessão do usuário. O tempo entre as verificações do dispositivo é configurável para melhorar o desempenho e permitir que essas verificações ocorram em partes de alto valor da sessão.

Como o problema ocorre

Os hackers querem explorar o caminho mais fácil para forçar a entrada em um sistema. Com a adoção crescente de outras tecnologias de autenticação, é mais difícil roubar credenciais de logon, portanto, os fraudadores estão procurando maneiras novas e criativas de entrar em um fluxo de transação autenticada válida. É esperado que essa exploração continue a crescer a uma taxa mais rápida no futuro.

Credenciais mais fortes podem ser usadas à medida que as empresas tentam impedir que um hacker roube um cookie de sessão. Credencias de dois fatores entregues como CA Strong Authentication podem ajudar a aumentar a segurança na porta de entrada, mas, com credenciais de um único fator, como nome de usuário/senha do Active Directory (AD), a questão é o quanto a segurança do aplicativo é boa DEPOIS de a sessão ter sido roubada. Usar informações com base na rede pode ser útil, mas vários dispositivos de rede podem falsificar ou ocultar endereços IP.

O Enhanced Session Assurance with DeviceDNA/Continuous Authentication da CA Technologies representa uma etapa significativa para impedir a reprodução de uma sessão roubada.

Utilizando a tecnologia DeviceDNA pendente de patente, que está disponível no CA Risk Authentication, o CA Single Sign-On pode identificar o cliente e determinar se o dispositivo de acesso mudou no meio da sessão.

Em uma base periódica configurável, o CA Single Sign-On verificará novamente se o dispositivo atual do cliente é idêntico ao dispositivo que se conectou originalmente para iniciar a sessão. Se ocorrer uma inconsistência, haverá uma alta probabilidade de que um invasor sequestrou a sessão. Nesse caso, o aplicativo pode solicitar que o usuário se autentique novamente usando credenciais secundárias ou simplesmente desconectar o usuário com uma mensagem solicitando que ele reinicie a sessão. Esse recurso pode ser habilitado em cada aplicativo. Aplicativos diferentes podem ter diferentes taxas de nova verificação com base no valor do ativo que está sendo protegido ou acessado.

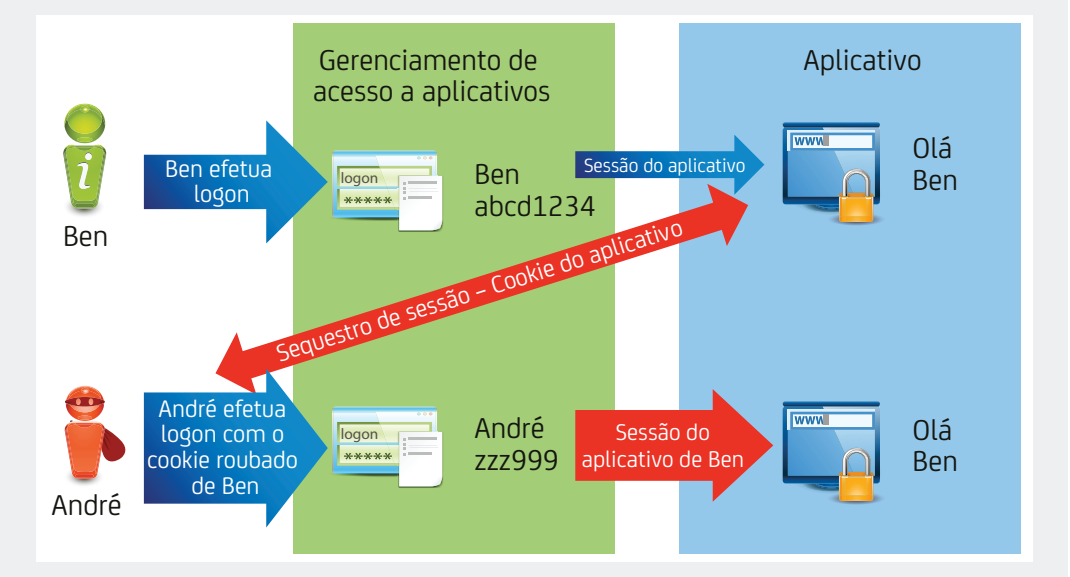
O gráfico a seguir descreve como ocorre o sequestro de sessão e a ameaça resultante para o aplicativo corporativo.

Etapa 1: Ben, o usuário legítimo, faz logon e é autenticado para o aplicativo.

Etapa 2: André, o fraudador, rouba as credenciais do cookie de sessão de Ben.

Etapa 3: André faz logon usando as credencias do cookie de sessão de Ben. O aplicativo pensa que ele é Ben, sabe que ele é um usuário legítimo e concede o mesmo acesso a ele.

Figura A.



Seção 2

Estendendo a garantia de sessão contínua para o aplicativo

O CA Access Gateway oferece outro recurso que pode estender essa segurança para a sessão do CA Single Sign-On até a sessão do aplicativo também. O recurso Vinculador de sessão foi desenvolvido para examinar as solicitações de entrada para validar se os cookies de sessão dos aplicativos são usados apenas em conjunto com a sessão do CA Single Sign-On para a qual foram criados. Se o Vinculador de sessão detectar que um usuário está apresentando um cookie de aplicativo de outro usuário e sua própria sessão do CA Single Sign-On (para tentar passar pelas verificações de garantia de sessão), o usuário será desconectado. É possível usar esse recurso de Vinculação de sessão combinado com o Enhanced Session Assurance with DeviceDNA para proteger cookies de aplicativos ou até mesmo os tokens de outras soluções WAM que não são do CA Single Sign-on.

Seção 3

Conclusão

O sequestro de sessão não é um novo risco de segurança, ele já era possível desde o HTTP 1.1. No entanto, seu perfil foi aperfeiçoado recentemente, e as organizações estão cientes da necessidade de estabelecer medidas para combatê-lo.

A CA Technologies desenvolveu uma solução para resolver o sequestro de sessão que compara as credenciais válidas de um usuário final e o cookie de sessão interno com a impressão digital do dispositivo que foi usado para o logon inicial do usuário. O Enhanced Session Assurance with DeviceDNA fornece "autenticação contínua" e está disponível "pronto para uso" para usuários do CA Single Sign-On r12.52, além de ser o único produto desse tipo que pode ajudar a impedir o sequestro de sessão.

Seção 4

Definições

O que é o CA Single Sign-On?

As soluções de gerenciamento de acesso flexíveis do CA Single Sign-On são soluções de gerenciamento de acesso altamente escaláveis e flexíveis que fornecem logon único seguro, autorização com base em diretivas, auditoria e administração para aplicativos web e na nuvem. O CA Federation dá suporte à federação de identidades com base em padrões para permitir que os usuários acessem aplicativos de maneira segura entre domínios. Ele ajuda a tornar sua presença online segura, disponível e acessível, sem interferência dos limites organizacionais. E o CA Access Gateway oferece um gateway de proxy que fornece um modelo de implementação opcional na família de SSO seguro e gerenciamento de acesso flexível para habilitar negócios online e logon único seguros.

O que é o CA Advanced Authentication?

O CA Advanced Authentication é uma solução flexível e escalável que incorpora métodos de autenticação com base em riscos, como identificação de dispositivos, geolocalização e atividades do usuário, além de uma ampla variedade de credenciais de autenticação forte multifator. Essa solução pode permitir que a organização crie o processo de autenticação adequado para cada aplicativo ou transação. Ela pode ser entregue como um software no local ou como um serviço na nuvem, protegendo o acesso aos aplicativos a partir de uma variedade de terminais, incluindo todos os dispositivos móveis populares. Essa solução abrangente pode permitir que sua organização aplique de forma econômica o método apropriado de autenticação forte entre ambientes, sem sobrecarregar os usuários finais.

O **CA Strong Authentication** é um servidor de autenticação versátil que permite que você implemente e aplique um grande intervalo de métodos de autenticação forte de uma maneira eficiente e centralizada. Ele permite interação online segura com seus funcionários, clientes e cidadãos fornecendo autenticação forte multifator para aplicativos internos e com base na nuvem. Ele inclui aplicativos de autenticação móvel e SDKs, além de várias formas de autenticação fora de banda.

O **CA Risk Authentication** oferece à sua organização a autenticação multifator que pode detectar e bloquear fraudes em tempo real, sem nenhuma interação com o usuário. Ele se integra com qualquer aplicativo online, incluindo sites/portais e VPNs e analisa o risco de transações e tentativas de acesso online. Essa forma de autenticação multifator, que é invisível para o usuário final, utiliza fatores contextuais, como ID do dispositivo, geolocalização, endereço IP e informações de atividades dos usuários para calcular uma pontuação de risco e recomendar a ação apropriada.

O **DeviceDNA** identifica os dispositivos que estão acessando seus aplicativos. Informações resumidas sobre a natureza do dispositivo, como o tipo e a ID exclusiva do dispositivo, são fornecidas para que o nível de risco possa ser avaliado.

Seção 5

Para obter mais informações

A Vinculação de sessão é discutida mais detalhadamente em uma documentação técnica adicional da CA Technologies intitulada "Vinculação de sessão e garantia de sessão".

Seção 6

Sobre o autor

Martin Yam é consultor estratégico da CA Technologies. Antes de ingressar na CA Technologies, Yam foi vice-presidente de vendas internacionais da Arcot Systems, Inc. Yam também ocupou funções de gerente executivo e de vendas na Oracle, Informix, Accrue Software, ParcPlace Systems e NeXT.

Conecte-se com a CA Technologies em ca.com/br

A CA Technologies (NASDAQ: CA) cria software que acelera a transformação das empresas e permite que elas aproveitem as oportunidades da era dos aplicativos. O software está no cerne de todas as empresas, em todos os setores. Do planejamento ao desenvolvimento e do gerenciamento à segurança, a CA está trabalhando com empresas de todo o mundo para mudar a maneira como vivemos, fazemos negócios e nos comunicamos – usando dispositivos móveis, as nuvens privada e pública e os ambientes distribuídos e de mainframe. Obtenha mais informações em **ca.com/br**.

1 O URL completo é 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 janeiro de 2014.

CS87229_0914