LIVRE BLANC | DÉCEMBRE 2014

Résolution de la plus grande brèche de sécurité dans la livraison d'applications Web

Prévention du risque de vol de session grâce au contrôle de session amélioré de CA Single Sign-On avec DeviceDNA™

Martin Yam
Équipe de gestion de la sécurité CA Technologies

ca technologies

Résumé

Défi

Depuis le début de la livraison d'applications Web, les fraudeurs ont la possibilité d'intercepter une transaction et d'usurper l'identité de l'utilisateur légitime. Les informations d'identification utilisées dans le cadre de cette fraude étant valides et l'utilisateur réel étant supposé en conserver le contrôle, il est difficile pour ne pas dire impossible de détecter et d'interrompre ce type d'usurpation d'identité.

Solution

La menace d'un vol de session (« session hijacking ») préoccupe de plus en plus les entreprises qui souhaitent protéger leurs actifs tout en offrant un accès aisé et sécurisé à leurs utilisateurs. Constituant l'un des principaux problèmes de sécurité auquel les entreprises sont confrontées aujourd'hui, le vol de session est décrit par de nombreux experts réputés comme un risque de sécurité quasi permanent (voir Wikipedia.org).

Il figure dans la liste des 10 principales vulnérabilités publiée en 2013 par l'OWASP (Open Web Application Security Project)[1]. Les deux catégories mentionnées ci-après constituent des cas spécifiques d'une authentification faible et d'un vol de session.

1. A2 – Violation de gestion d'authentification et de session
2. A3 – Scripts intersites (XSS)

Ceci souligne la grande visibilité de ce problème et la nécessité de développer un meilleur système de protection.

Avantages

Pour contrer ce problème de sécurité, CA Technologies a mis au point une solution compatible avec tous les logiciels standard (COTS) et toutes les applications WAM personnalisées en liant les informations d'identification valides de l'utilisateur et le cookie de la session à l'empreinte de l'appareil sur lequel l'utilisateur s'est connecté initialement. Le contrôle périodique et la validation de la combinaison informations d'identification/de l'appareil pendant une opération permettent de vérifier que c'est bien l'utilisateur réel qui poursuit la transaction.

Section 1

Importance d'une « authentification continue »

Loin d'être nouveau, le vol de session, également appelé vol de cookie, s'est transformé en risque de sécurité quasi permanent depuis l'instauration de la norme HTTP 1.1. Un rapport récent de Forrester Research sur l'authentification continue reconnaît, de notre point de vue, la menace résultant du vol de session. Le numéro quatre de l'étude « OUR PREDICTIONS FOR IAM IN 2014 » [2] de Forrester Research précise :

L'authentification continue protège les sessions de bout en bout. *Les adresses IP, les ID d'appareil ou leur réputation n'offrent plus une protection suffisante contre les menaces car ces paramètres affectent principalement la première étape des interactions utilisateur : l'authentification initiale. Une fois l'utilisateur connecté, la protection est minimale. Avec l'authentification continue, il est possible d'étudier le comportement de l'utilisateur (principalement sur le Web lors de la première phase, puis sur tous les canaux lors des phases ultérieures) pour déterminer si sa navigation est rationnelle. Au moindre doute (agent de l'utilisateur sondant très rapidement le site ou suspicion d'une attaque ou d'une exfiltration de données), la solution peut alerter les administrateurs, voire interrompre la session.*

Ce que vous devez savoir. *Pour vous prémunir des sessions suspectes, vous devez poser les bases d'un bon comportement. Pour ce faire, demandez à votre fournisseur de solution d'authentification basée sur les risques (RBA) s'il est en mesure d'instaurer une activité utilisateur de référence avant l'exécution des opérations de routine car l'obtention de ces informations par tout autre moyen est quasiment impossible.*

Pour garantir une « authentification continue », CA Technologies propose un contrôle de session amélioré avec DeviceDNA et prêt à l'emploi pour les utilisateurs de CA Single Sign-On r12.52. Grâce à « l'outil de liaison de sessions » de CA Single Sign-On, il est également possible d'étendre cette fonctionnalité pour protéger des applications qui utilisent leurs propres cookies de session, comme Tivoli Access Manager, Oracle Access Manager ou d'autres solutions développées en interne, sans devoir apporter la moindre modification à ces applications.

Le contrôle de session amélioré avec DeviceDNA tire parti des composants de solution CA Technologies existants. Il repose sur la capacité de CA Risk Authentication à identifier et à collecter des caractéristiques de l'appareil de l'utilisateur légitime à partir de la séquence de connexion initiale et de les comparer périodiquement à l'appareil réel utilisant le cookie de session pendant la session de l'utilisateur. L'intervalle entre les contrôles de l'appareil est configurable pour améliorer les performances. Il est en outre possible de veiller à ce que ce contrôle se produise aux moments critiques de la session.

Apparition du problème

Les pirates cherchent à exploiter le chemin d'accès à un système le plus facile. Du fait de l'adoption d'autres technologies d'authentification qui tend à se généraliser, il est de plus en plus difficile de s'approprier frauduleusement des informations d'identification. Les fraudeurs cherchent donc de nouvelles manières créatives d'accéder à un flux de transaction authentifié et valide. Ce type de fraude devrait donc prendre de plus en plus d'ampleur à l'avenir.

Les entreprises qui tentent d'empêcher un pirate de voler un cookie de session peuvent recourir à des informations d'identification forte. Si l'authentification à deux facteurs de CA Strong Authentication peut faciliter l'instauration d'un système de sécurité en entrée, avec des informations d'identification à un facteur comme le nom d'utilisateur/mot de passe d'Active Directory (AD), la question serait plutôt de savoir dans quelle mesure l'application est sécurisée UNE FOIS la session usurpée. Il peut être intéressant d'utiliser des informations basées sur le réseau, mais le recours à divers périphériques réseau peut facilement imiter ou masquer des adresses IP.

Le contrôle de session amélioré avec DeviceDNA/l'authentification continue de CA Technologies représente un pas en avant significatif en matière de prévention des usurpations de session à répétition.

En tirant parti de la technologie DeviceDNA en instance de brevet, intégrée à CA Risk Authentication, CA Single Sign-On peut identifier le client et déterminer si le périphérique d'accès a changé pendant la session.

CA Single Sign-On revérifiera régulièrement, suivant un intervalle de temps configurable, que l'appareil client actuel est identique à celui utilisé pour ouvrir initialement la session. Si une discordance est détectée, il est fort probable qu'un pirate ait usurpé la session. Le cas échéant, l'application peut demander à l'utilisateur de s'authentifier à nouveau à l'aide d'autres informations d'identification ou le déconnecter tout simplement en l'invitant à redémarrer la session. Il est possible de configurer cette fonctionnalité application par application, de manière à utiliser des intervalles de contrôle différents, en fonction de la valeur des actifs à protéger ou consulter.

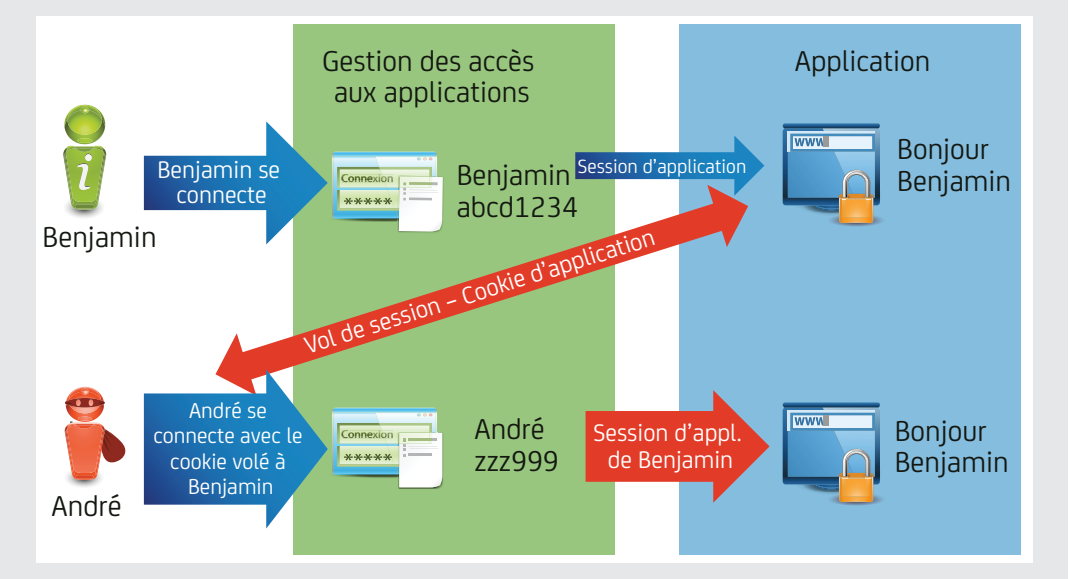
L'illustration ci-après décrit le processus de vol de session et la menace qui en résulte pour l'application de l'entreprise.

Étape 1 : Benjamin, l'utilisateur légitime, se connecte et s'authentifie auprès de l'application.

Étape 2 : André, le fraudeur, vole les informations d'identification du cookie de session de Benjamin.

Étape 3 : André se connecte à présent avec les informations d'identification du cookie de session de Benjamin ; l'application pense qu'il s'agit de Benjamin et le reconnaissant comme utilisateur légitime, octroie à André les mêmes droits d'accès.

Illustration A.



Section 2

Extension du contrôle de session continu à l'application

CA Access Gateway propose une autre fonctionnalité susceptible d'étendre la sécurité de la session CA Single Sign-On à la session de l'application. L'outil de liaison de sessions est conçu pour analyser les requêtes entrantes afin de s'assurer que les cookies de session des applications sont uniquement utilisés avec la session CA Single Sign-On pour laquelle ils ont été créés. Si cet outil détecte qu'un utilisateur présente un cookie d'application d'un autre utilisateur sur sa propre session CA Single Sign-On (et essaie ainsi de contourner les contrôles de session), il le déconnecte. Cette fonctionnalité peut être combinée au contrôle de session amélioré avec DeviceDNA pour renforcer la sécurité des cookies d'application ou les jetons de solutions WAM différentes de CA Single Sign-On.

Section 3

Conclusion

Le vol de session n'est pas un nouveau risque en matière de sécurité. Il existe depuis l'apparition de la norme HTTP 1.1. Cette menace a toutefois pris de l'ampleur récemment et les organisations sont conscientes qu'elles doivent prendre des mesures pour y faire face.

CA Technologies a développé une solution de prévention du vol de session qui compare les informations d'identification valides de l'utilisateur final et le cookie de session interne de l'appareil avec l'empreinte de l'appareil utilisé pour l'ouverture initiale de la session de l'utilisateur. Le contrôle de session amélioré avec DeviceDNA propose une « authentification continue » et est prêt à l'emploi pour les utilisateurs de CA Single Sign-On r12.52. Cette solution de prévention du vol de session est unique en son genre.

Section 4

Définitions

Présentation de CA Single Sign-On

Les solutions de gestion des accès flexibles CA Single Sign-On sont hautement évolutives. Elles offrent des fonctionnalités d'authentification unique, d'autorisation basée sur des règles, d'audit et d'administration des applications Web et Cloud. CA Federation prend en charge la fédération des identités basée sur des normes pour permettre aux utilisateurs d'accéder aux applications en toute sécurité, indépendamment du domaine. Votre présence en ligne est sécurisée et accessible au-delà des locaux de l'entreprise. La passerelle proxy hautement performante CA Access Gateway propose un modèle de déploiement facultatif. Cette solution du panel de gestion des accès flexibles et à authentification unique permet de sécuriser l'activité en ligne et l'authentification unique.

Présentation de CA Advanced Authentication

CA Advanced Authentication est une solution flexible et évolutive qui incorpore des méthodes d'authentification basées sur les risques comme l'identification de périphériques, la géolocalisation et l'activité des utilisateurs, ainsi que de nombreuses autres informations d'authentification forte multifacteur. Cette solution peut notamment permettre à l'organisation de créer un processus d'authentification approprié à chaque application ou opération. Disponible sous forme de logiciel à déployer sur site ou en tant que service Cloud, elle permet de protéger l'accès aux applications depuis une multitude de terminaux, notamment tous les appareils mobiles les plus courants. Cette solution complète peut permettre à votre organisation de mettre en place à moindre coût la méthode d'authentification forte appropriée sur l'ensemble de vos environnements sans gêner les utilisateurs finaux.

CA Strong Authentication est un serveur d'authentification polyvalent qui vous permet de déployer et d'appliquer de nombreuses méthodes d'authentification forte de manière efficace et centralisée. Il offre une interaction en ligne sécurisée avec vos employés, clients et utilisateurs grâce à une authentification forte multifacteur compatible avec les applications internes et Cloud. Il inclut des applications d'authentification mobile et des kits de développement logiciel (SDK), ainsi que plusieurs formes d'authentification hors bande.

CA Risk Authentication propose une authentification multifacteur capable de détecter et bloquer les fraudes en temps réel, sans interaction avec l'utilisateur. Cet outil s'intègre avec toutes les applications en ligne (y compris les sites et portails Web, ainsi que les VPN) et analyse les risques liés aux tentatives d'accès en ligne et aux transactions. Cette forme d'authentification multifacteur, totalement invisible pour l'utilisateur final, repose sur des facteurs contextuels comme l'ID de l'appareil, la géolocalisation, l'adresse IP et des informations relatives à l'activité de l'utilisateur, pour calculer le niveau de risque et recommander l'action appropriée.

DeviceDNA identifie les appareils autorisés à accéder à vos applications. Des informations récapitulatives sur la nature de l'appareil, comme son type et son ID unique, sont également fournies afin de pouvoir évaluer le niveau de risque.

Section 5

Pour plus d'informations

L'outil de liaison de sessions est présenté plus en détails dans le livre blanc de CA Technologies intitulé « Session Linking and Session Assurance ».

Section 6

À propos de l'auteur

Martin Yam occupe le poste de conseiller stratégique au sein de CA Technologies. Avant de rejoindre CA Technologies, il a été vice-président du département commerce international d'Arcot Systems, Inc. Il a également travaillé comme cadre et responsable commercial chez Oracle, Informix, Accrue Software, ParcPlace Systems et NeXT.

Restez connecté à CA Technologies sur ca.com/fr

CA Technologies (NASDAQ : CA) crée des logiciels qui alimentent la transformation des entreprises et leur permettent de saisir toutes les opportunités de l'économie des applications. Le logiciel est au cœur de chaque activité et de chaque industrie. De la planification au développement, en passant par la gestion et la sécurité, CA Technologies collabore avec des entreprises partout dans le monde afin de transformer la façon dont nous vivons, interagissons et communiquons, dans les environnements mobiles, de Cloud public et privé, distribués et mainframe. Pour en savoir plus, rendez-vous sur **ca.com/fr**.

1 URL complète : 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 janvier 2014.

CS87229_0914