WHITE PAPER | DEZEMBER 2014

Schließen der größten Security-Lücke bei der Bereitstellung von Webanwendungen

Bekämpfen von Session Hijacking mit CA Single Sign-On Enhanced Session Assurance with DeviceDNA™

Martin Yam
CA Security Management-Team

ca technologies

Kurzfassung

Ausgangssituation

Seit den Anfängen der Bereitstellung von Webanwendungen hat es die Gelegenheit für Betrüger gegeben, sich in eine Transaktion einzuklinken und sich als legitimer Benutzer auszugeben. Da die für diesen Betrug verwendeten Anmeldeinformationen gültig sind und „angenommen wird, dass sie der Kontrolle des echten Benutzers unterliegen", war es stets schwierig oder unmöglich, diese Art der vorgeblichen Identität zu erkennen und abzuwehren.

Chancen

Die Bedrohung des „Session Hijacking" bedeutet wachsende Sorgen für Unternehmen, die Assets schützen und ihren Benutzern zugleich einfachen, aber sicheren Zugriff bieten müssen. Sie ist heute eines der größten Security-Probleme für Unternehmen. Viele führende Experten identifizieren „Session Hijacking" als ein fast permanentes Security-Risiko (siehe Wikipedia.org).

Das Open Web Application Security Project (OWASP) weist in seiner Top 10-Liste für 2013 auf diese Schwachstelle hin[1]. Die beiden unten aufgeführten Kategorien sind Spezialfälle von schlechter Authentifizierung und Session Hijacking.

1. A2 – Fehlerhafte Authentifizierung und fehlerhaftes Session Management
2. A3 – Cross-Site Scripting (XSS)

Dies weist auf die hohe Sichtbarkeit dieses Problems hin und bedeutet, dass eine Lösung, die ihm begegnen kann, weit wertvoller ist.

Nutzen

CA Technologies hat eine Lösung für dieses Security-Problem entwickelt, die alle kommerziell erhältlichen sowie selbst entwickelten Lösungen für das Web Access Management (WAM) abdeckt, indem sie die gültigen Anmeldeinformationen des Benutzers sowie das Session-Cookie mit dem elektronischen Fingerabdruck des Geräts verbindet, das für die anfängliche Benutzeranmeldung verwendet wurde. Indem die Lösung diese Kombination aus Anmeldeinformationen und Gerät während einer Transaktions-Session regelmäßig überprüft, kann sie sicherstellen, dass der tatsächliche Benutzer seine Transaktion fortsetzt und dass kein Session Hijacking stattgefunden hat.

Abschnitt 1

Die Wichtigkeit der „kontinuierlichen Authentifizierung“

Session Hijacking, auch als Cookie Hijacking bezeichnet, ist keine neue Bedrohung, sondern hat sich zu einem fast permanenten Security-Risiko entwickelt, seit HTTP 1.1 zum Standard wurde. In einem aktuellen Bericht von Forrester Research wird die „kontinuierliche Authentifizierung“ erörtert. Aus unserer Perspektive hebt dies die Bedrohung durch Session Hijacking hervor. Die vierte der Vorhersagen von Forrester Research für IAM im Jahr 2014 lautet[2]:

Mit der kontinuierlichen Authentifizierung werden Sessions von Anfang bis Ende geschützt: *Die Verwendung von IP-Adressen – oder Geräte-IDs und -Reputation – bedeutet keinen ausreichenden Schutz vor Bedrohungen mehr, da diese Parameter sich im Wesentlichen nur auf den ersten Schritt in Benutzerinteraktionen auswirken: Authentifizierung an der Eingangstür. Sobald der Benutzer angemeldet ist, bieten sie kaum Schutz. Hier setzt die kontinuierliche Authentifizierung an: Sie überwacht das Benutzerverhalten (in der ersten Phase vor allem auf dem Web-Channel, in späteren Phasen auf anderen Channels), um zu ermitteln, ob der Benutzer ordnungsgemäß auf der Seite navigiert. Wenn es Grund zur Beunruhigung gibt — der Agent des Benutzers erfasst die Seite mit hoher Geschwindigkeit, oder es ist zu vermuten, dass ein Angriff vorliegt oder dass Daten nach außen dringen — kann die Lösung Administratoren benachrichtigen und optional sogar die Session beenden.*

Was Sie tun müssen: *Um sich gegen verdächtige Sessions zu schützen, müssen Sie ein gutes Grundverhalten einrichten. Bitten Sie den Anbieter Ihrer Lösung für die risikobasierte Authentifizierung (RBA), ein Grundverhalten für die Benutzeraktivitäten einzurichten, bevor der Routinebetrieb beginnt – da es fast unmöglich ist, diese Informationen auf andere Weise zu erhalten.*

CA Technologies bietet Enhanced Session Assurance with DeviceDNA, um „kontinuierliche Authentifizierung“ bereitzustellen; die Lösung ist sofort einsatzfähig für Benutzer von CA Single Sign-On r12.52. Über eine andere Funktion von CA Single Sign-On, die als „Session Linking“ bezeichnet wird, kann diese Funktion auch auf den Schutz von Anwendungen erweitert werden, die ihre eigenen Session-Cookies verwenden, wie Tivoli Access Manager, Oracle Access Manager oder viele selbst entwickelte Lösungen. Beachten Sie, dass dies möglich ist, ohne dass an diesen anderen Anwendungen Änderungen vorgenommen werden müssen.

Enhanced Session Assurance with DeviceDNA nutzt vorhandene Lösungskomponenten von CA Technologies und verwendet CA Risk Authentication, um Gerätemerkmale des legitimen Benutzers aus seiner anfänglichen Anmeldesequenz zu identifizieren und zu erfassen und sie regelmäßig mit dem tatsächlichen Gerät zu vergleichen, das das Session Cookie während der Session des Benutzers verwendet. Wie viel Zeit zwischen den Geräteprüfungen vergeht, kann konfiguriert werden, um die Performance zu verbessern und diese Überprüfungen in besonders wichtigen Teilen der Session durchzuführen.

Wie das Problem auftritt

Hacker möchten den einfachsten Weg nutzen, in ein System einzubrechen.
Da andere Authentifizierungstechnologien zunehmend eingeführt werden, wird es schwieriger, Anmeldeinformationen zu stehlen, sodass Betrüger neue und kreative Möglichkeiten finden, in einen gültigen, authentifizierten Transaktionsfluss einzudringen. Es wird erwartet, dass dieser Exploit in Zukunft schneller zunehmen wird.

Strengere Anmeldeinformationen können verwendet werden, wenn Unternehmen versuchen, Hacker am Stehlen von Session Cookies zu hindern. Zwei-Faktor-Anmeldeinformationen, die als CA Strong Authentication bereitgestellt werden, können zur Security „an der Eingangstür" beitragen, aber mit Ein-Faktor-Anmeldeinformationen, wie Benutzernamen und Passwort von Active Directory (AD), besteht die Herausforderung darin, wie gut die Anwendungs-Security ist, NACHDEM die Session gestohlen wurde. Die Verwendung netzwerkbasierter Informationen kann nützlich sein, aber verschiedene Netzwerkgeräte können IP-Adressen leicht vortäuschen (Spoofing) oder verbergen.

Enhanced Session Assurance with DeviceDNA/Continuous Authentication von CA Technologies bedeutet einen wichtigen Schritt nach vorn, um die Wiedergabe gestohlener Sessions zu verhindern.

Durch Nutzung der zum Patent angemeldeten DeviceDNA-Technologie, die in CA Risk Authentication zur Verfügung steht, kann CA Single Sign-On den Client identifizieren und ermitteln, ob das zugreifende Gerät während der Session gewechselt wurde.

In konfigurierbaren, regelmäßigen Abständen überprüft CA Single Sign-On erneut, ob das aktuelle Clientgerät identisch mit dem Gerät ist, das sich ursprünglich angemeldet hat, um die Session zu beginnen. Wenn eine Abweichung auftritt, ist es sehr wahrscheinlich, dass ein Angreifer ein Session Hijacking durchgeführt hat. In diesem Fall kann die Anwendung anfordern, dass der Benutzer sich mit sekundären Anmeldeinformationen erneut authentifiziert, oder sie kann den Benutzer einfach abmelden und ihn auffordern, die Session neu zu starten. Diese Funktion kann für jede Anwendung einzeln aktiviert werden. Unterschiedliche Anwendungen können in unterschiedlichen Abständen erneut überprüft werden, abhängig vom Wert des Assets, auf das der Zugriff geschützt wird.

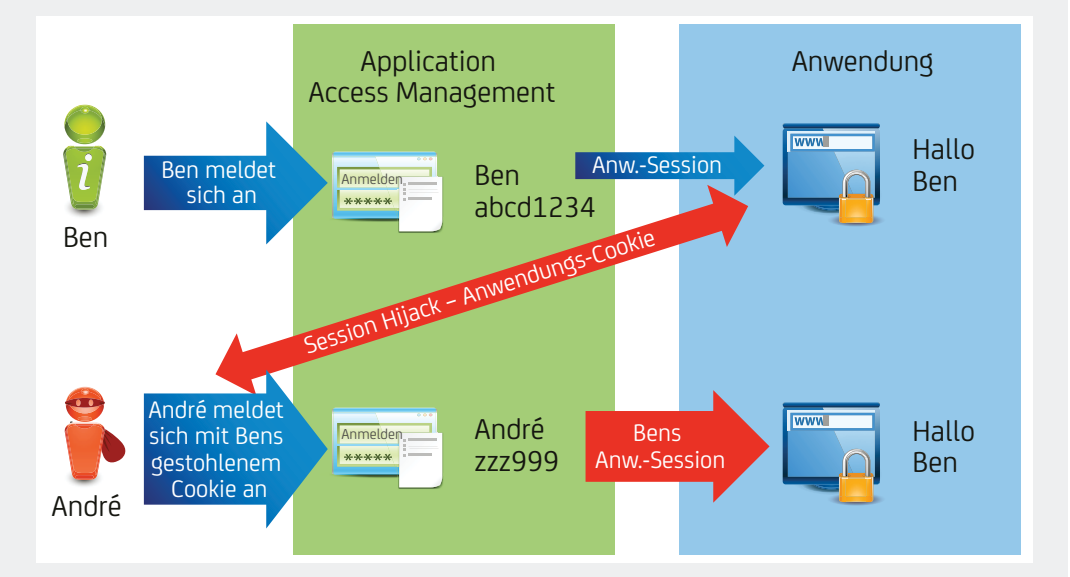
Die folgende Grafik zeigt, wie Session Hijacking auftritt und wie es die Unternehmensanwendung bedroht.

Schritt 1: Ben, der legitime Benutzer, meldet sich an und wird für die Anwendung authentifiziert.

Schritt 2: André, der Betrüger, stiehlt Bens Session Cookie-Anmeldeinformationen.

Schritt 3: André meldet sich jetzt mit Bens Session Cookie-Anmeldeinformationen an; die Anwendung hält ihn für Ben, den legitimen Benutzer, und gewährt ihm den gleichen Zugriff.

Abbildung A.



ca technologies

Abschnitt 2

Erweitern der kontinuierlichen Session Assurance in die Anwendung

CA Access Gateway bietet eine weitere Funktion, die diese Security für die Session von CA Single Sign-On bis hin zur Session der Anwendung erweitern kann. Die Funktion Session Linker wurde dafür entwickelt, eingehende Anforderungen zu untersuchen, um sicherzustellen, dass Session Cookies von Anwendungen nur in Verbindung mit der Session von CA Single Sign-On verwendet werden, für die sie erstellt wurden. Wenn Session Linker erkennt, dass ein Benutzer ein Anwendungs-Cookie eines anderen Benutzers und seine eigene Session von CA Single Sign-On vorlegt (in dem Versuch, die Überprüfungen der Session Assurance zu umgehen), wird der Benutzer abgemeldet. Die Funktion Session Linking kann in Kombination mit Enhanced Session Assurance with DeviceDNA verwendet werden, um Anwendungs-Cookies oder sogar die Tokens anderer Lösungen für das Single Sign-On Web Access Management (WAM), die nicht von CA Technologie stammen, zu sichern.

Abschnitt 3

Schlussfolgerung

Session Hijacking ist kein neues Security-Risiko, sondern seit HTTP 1.1 möglich. Es ist jedoch in der letzten Zeit viel kritischer geworden, und Organisationen sind sich darüber bewusst, dass sie Gegenmaßnahmen ergreifen müssen.

CA Technologies hat eine Lösung zur Abwehr des Session Hijacking entwickelt, die die gültigen Anmeldeinformationen und das interne Session Cookie eines End Users mit dem elektronischen Fingerabdruck des Geräts vergleicht, das für die anfängliche Benutzeranmeldung verwendet wurde. Enhanced Session Assurance with DeviceDNA bietet „kontinuierliche Authentifizierung“, ist sofort einsatzfähig für Benutzer von CA Single Sign-On r12.52 und ist das einzige Produkt seiner Art, das Session Hijacking verhindern kann.

Abschnitt 4

Definitionen

Was ist CA Single Sign-On?

Lösungen mit CA Single Sign-On für das flexible Access Management sind hoch skalierbar. Sie bieten sicheres Single Sign-On, richtlinienbasierte Autorisierung, Auditing und Verwaltung für Web- und Cloud-Anwendungen. CA Federation unterstützt die auf Standards basierende Identity Federation, damit Benutzer sicher auf Anwendungen in allen Bereichen zugreifen können. Die Lösung trägt dazu bei, dass Ihre Online-Präsenz sicher und verfügbar ist und dass Sie auf sie zugreifen können – ohne dass Organisationsgrenzen Hindernisse darstellen. CA Access Gateway bietet ein leistungsstarkes Proxy-Gateway, das innerhalb der Produktfamilie für sicheres SSO und flexibles Access Management ein optionales Bereitstellungsmodell für sichere Online-Geschäftsvorgänge und Single Sign-On bereitstellt.

Was ist CA Advanced Authentication?

CA Advanced Authentication ist eine flexible und skalierbare Lösung, die sowohl risikobasierte Authentifizierungsmethoden wie Geräteerkennung, geografischen Standort und Benutzeraktivität als auch eine Vielzahl sicherer Mehrfaktor-Authentifizierungsnachweise umfasst. Mit dieser Lösung kann die Organisation den geeigneten Authentifizierungsprozess für jede Anwendung oder Transaktion erstellen. Sie kann als On-Premise-Software oder als Cloud-Service bereitgestellt werden, und sie kann den Anwendungszugriff über zahlreiche unterschiedliche Endpunkte schützen, einschließlich aller verbreiteten Mobile Devices. Mit dieser umfassenden Lösung kann Ihre Organisation kosteneffektiv die geeignete Methode für die strenge Authentifizierung in allen Umgebungen erzwingen, ohne die End User zu belasten.

CA Strong Authentication ist ein vielseitiger Authentifizierungsserver, mit dem Unternehmen ein breites Spektrum an strengen Authentifizierungsverfahren kostengünstig und zentralisiert implementieren können. Er ermöglicht sichere Online-Interaktionen mit Ihren Mitarbeitern, Kunden und Bürgern, indem eine strenge Mehrfaktor-Authentifizierung sowohl für interne Anwendungen als auch für Cloud-basierte Anwendungen bereitgestellt wird. Dieser Server umfasst mobile Authentifizierungsanwendungen und SDKs sowie verschiedene Formen der Out-of Band-Authentifizierung.

CA Risk Authentication bietet Ihrem Unternehmen Mehrfaktor-Authentifizierung, die Betrug in Echtzeit erkennen und blockieren kann, ohne jegliche Interaktion mit dem Benutzer. Diese Lösung kann in jede Online-Anwendung integriert werden, einschließlich Websites/Portale und VPNs, und analysiert das Risiko von Online-Zugriffsversuchen und -Transaktionen. Diese Form der Mehrfaktor-Authentifizierung, die für den End User nicht sichtbar ist, verwendet kontextbezogene Faktoren, wie z. B. Geräte-ID, geografischen Standort, IP-Adresse und Informationen zur Benutzeraktivität, um Risikowerte zu berechnen und entsprechende Maßnahmen zu empfehlen.

DeviceDNA identifiziert Geräte, die auf Ihre Anwendungen zugreifen. Zusammenfassende Informationen zur Art des Geräts, wie Gerätetyp und eindeutige Geräte-ID, werden bereitgestellt, damit das Risiko-Level eingeschätzt werden kann.

Abschnitt 5

Weitere Informationen

Session Linking wird in einem ergänzenden White Paper von CA Technologies mit dem Titel „Session Linking und Session Assurance“ detaillierter behandelt.

Abschnitt 6

Informationen zum Autor

Martin Yam ist Strategic Advisor bei CA Technologies. Bevor er zu CA Technologies kam, war Martin Yam Vice President of Worldwide Sales bei Arcot Systems, Inc. Yam hat außerdem in Führungs- und Vertriebsmanagementpositionen bei Oracle, Informix, Accrue Software, ParcPlace Systems und NeXT gearbeitet.

Mit CA Technologies vernetzen unter ca.com/de

CA Technologies (NASDAQ: CA) entwickelt Software, die Unternehmen bei der Umstellung auf die Application Economy unterstützt. Software steht im Mittelpunkt jedes Unternehmens in allen Branchen. Von der Planung über die Entwicklung bis zum Management und der Security – CA Technologies arbeitet weltweit mit Unternehmen zusammen, um die Art, wie wir leben, Transaktionen durchführen und kommunizieren, mit zu verändern, ganz gleich, ob in mobilen, privaten und öffentlichen Cloud-Umgebungen oder in verteilten Systemen und Mainframe-Umgebungen. Weitere Informationen finden Sie unter **ca.com/de**.

1 Die vollständige URL lautet 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. Januar 2014.

CS87229_0914