WHITE PAPER | DICEMBRE 2014

Risolvere il principale problema di sicurezza nel Web Application Delivery

Gestione dell'hijack della sessione con CA Single Sign-On Enhanced Session Assurance con DeviceDNA™

Martin Yam
CA Security Management Team

ca technologies

Riepilogo esecutivo

Sfida

Fin dall'inizio del web application delivery, i truffatori hanno avuto l'occasione di entrare nel bel mezzo di una transazione e agire come utente legittimo. Poiché le credenziali utilizzate per questa frode sono valide e "previste per essere sotto il controllo dell'utente reale", è stato difficile, se non impossibile, fermare questo tipo di sostituzione di persona.

Opportunità

La minaccia di "hijack della sessione" è un argomento che desta sempre più preoccupazione tra le aziende con risorse da proteggere, ma che desiderano al contempo fornire un accesso semplice ma sicuro ai propri utenti. Si tratta di uno dei principali problemi di sicurezza che le aziende odierne devono affrontare. Molti esperti identificano "l'hijack della sessione" come un rischio per la sicurezza quasi permanente (consultare Wikipedia.org).

L'Open Web Application Security Project (OWASP) evidenzia questa vulnerabilità nella sua classifica Top 10 per il 2013[1]. Le due categorie elencate di seguito sono casi specifici di scarsa autenticazione e hijack della sessione.

1. A2 – Broken Authentication and Session Management
2. A3 – Cross-Site Scripting (XSS)

Ciò evidenzia l'elevata visibilità del problema e l'importanza di trovare una soluzione che possa risolverlo.

Vantaggi

CA Technologies ha sviluppato una soluzione a questo problema di sicurezza che unisce tutte le soluzioni commercial off-the-shelf (COTS) e Web Access Management (WAM) locali, collegando le credenziali valide dell'utente e i cookie di sessione alla device fingerprint utilizzata per l'accesso iniziale dell'utente. Controllando periodicamente questa combinazione di credenziali e device durante la sessione di una transazione e convalidandola, è possibile garantire che l'utente effettivo sta continuando la transazione e che non si è verificato un hijack della sessione.

Sezione 1

L'importanza "dell'autenticazione continua"

L'hijack della sessione, noto anche con il termine "cookie hijacking", non è una minaccia nuova e rappresenta di fatto un rischio per la sicurezza pressoché permanente da quando HTTP 1.1 è diventato uno standard. In un recente report di Forrester Research si parla dell'"autenticazione continua" che, dal nostro punto di vista, riconosce la minaccia costituita dall'hijack della sessione. Il punto quattro di "OUR PREDICTIONS FOR IAM IN 2014" [2] di Forrester Research è:

L'autenticazione continua proteggerà le sessioni dall'inizio alla fine. *L'utilizzo di indirizzi IP o ID device con relativa reputazione non è più sufficiente per proteggere dalle minacce, perché questi parametri interessano principalmente solo la prima fase delle interazioni degli utenti: l'autenticazione "front-door". Una volta che l'utente ha effettuato l'accesso, la protezione offerta è minima. L'autenticazione continua, osservando il comportamento dell'utente (in particolare sul canale web nella prima fase e su altri canali in quelle successive), consente di determinare se l'utente sta esplorando il sito in modo ordinato. Se è presente un motivo di allarme, ad esempio l'utente sta esplorando il sito ad alte velocità o si sospetta un attacco o l'estrazione di dati, la soluzione può avvisare gli amministratori e, ipoteticamente, persino terminare la sessione.*

Operazioni da eseguire. *Per proteggere il sistema da sessioni sospette, occorre stabilire una linea di base di comportamento corretta. Sarà necessario chiedere al fornitore della soluzione RBA (Risk-Based Authentication) di controllare se è possibile stabilire una linea di base dell'attività dell'utente prima dell'inizio delle operazioni ordinarie, perché ottenere queste informazioni in altri modi è quasi impossibile.*

CA Technologies offre un controllo della sessione migliorato grazie a DeviceDNA per fornire l'"autenticazione continua" ed è disponibile "out of the box" per gli utenti di CA Single Sign-On r12.52. Tramite un'altra caratteristica di CA Single Sign-On denominata "Session Linking", è possibile estendere questa funzionalità anche per proteggere applicazioni che utilizzano i propri cookie di sessione, come Tivoli Access Manager, Oracle Access Manager o molte soluzioni locali. È importante sottolineare che questa operazione può essere eseguita senza apportare modifiche alle altre applicazioni.

Enhanced Session Assurance con DeviceDNA sfrutta i componenti delle soluzioni CA Technologies esistenti. Utilizza la funzionalità inclusa in CA Risk Authentication per identificare e raccogliere le caratteristiche del device dell'utente legittimo dalla sequenza di accesso iniziale e le confronta periodicamente con il device effettivo su cui sono presenti i cookie di sessione durante la sessione dell'utente. È possibile configurare il tempo tra i controlli del device per migliorare le performance e consentire questo controllo in parti di valore elevato della sessione.

Come si verifica il problema

Gli hacker cercano la strada più semplice per irrompere in un sistema. Con la crescente adozione delle tecnologie di autenticazione, è sempre più difficile rubare le credenziali di accesso, pertanto i truffatori stanno cercando nuovi metodi creativi per inserirsi in un flusso di transazione valido e autenticato. Si prevede che questo codice exploit sarà sempre più impiegato in futuro.

Le aziende possono utilizzare credenziali più sicure per evitare che un hacker rubi un cookie di sessione. Le credenziali a due fattori fornite come CA Strong Authentication possono contribuire a migliorare la sicurezza front door, ma con credenziali a fattore singolo, come nome utente/password Active Directory (AD), la sfida è costituita dal livello di protezione dell'applicazione DOPO il furto della sessione. L'utilizzo di informazioni basate sulla rete può essere utile, ma vari device di rete possono facilmente nascondere o effettuare lo spoofing degli indirizzi IP.

Enhanced Session Assurance con DeviceDNA/Continuous Authentication di CA Technologies rappresenta un significativo passo avanti per la prevenzione della riproduzione di sessioni rubate.

Utilizzando la tecnologia DeviceDNA in attesa di brevetto, disponibile in CA Risk Authentication, CA Single Sign-On è in grado di identificare il client e determinare se il device che sta effettuando l'accesso è cambiato nel corso della sessione.

Su base periodica configurabile, CA Single Sign-On ricontrollerà che il device client corrente sia identico al device che ha eseguito l'accesso originariamente all'inizio della sessione. Se i device non corrispondono, è altamente probabile che si sia verificato un attacco con hijack della sessione. In questo caso, l'applicazione può richiedere all'utente di eseguire nuovamente l'autenticazione con le credenziali secondarie oppure può semplicemente disconnettere l'utente con un messaggio che richiede di riavviare la sessione. Questa funzionalità può essere attivata per singola applicazione. Diverse applicazioni possono avere livelli di ricontrollo differenti in base al valore della risorsa da proteggere o a cui si desidera accedere.

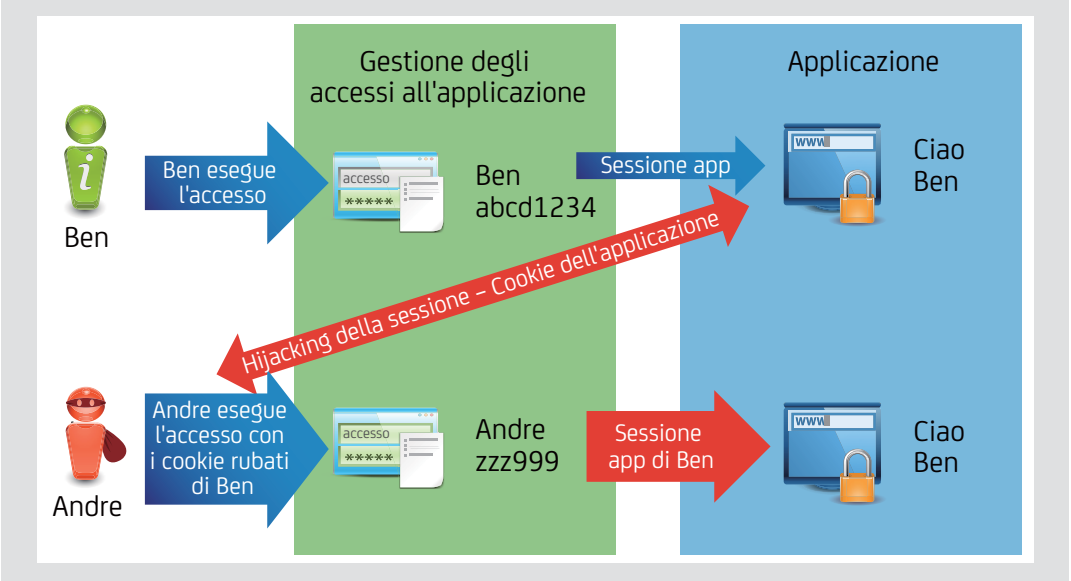
Il grafico seguente descrive come si verifica l'hijack della sessione e la conseguente minaccia per l'applicazione aziendale.

Fase 1: Ben, l'utente legittimo, accede all'applicazione ed è autenticato.

Fase 2: Andre, il truffatore, ruba le credenziali del cookie di sessione di Ben.

Fase 3: Andre ora accede utilizzando le credenziali del cookie di sessione di Ben; l'applicazione pensa che sia Ben ad effettuare l'accesso, sa che Ben è il legittimo utente e gli consente lo stesso accesso.

Figura A.



Sezione 2

Estensione di Continuous Session Assurance nell'applicazione

CA Access Gateway offre un'altra funzionalità in grado di aumentare questa sicurezza per la sessione CA Single Sign-On, nonché la sessione dell'applicazione. La funzionalità Session Linker è progettata per esaminare le richieste in arrivo e verificare che i cookie di sessione dalle applicazioni siano utilizzati solo insieme alla sessione CA Single Sign-On per cui sono stati creati. Se Session Linker rileva che un utente sta presentando un cookie applicazione da un utente diverso o che non coincide con la propria sessione di CA Single Sign-On (per provare a superare i controlli di session assurance), l'utente viene disconnesso. È possibile utilizzare questa funzionalità di Session Linking insieme a Enhanced Session Assurance con DeviceDNA per proteggere i cookie dell'applicazione o anche i token di altre soluzioni non-CA Single Sign-On Web Access Management (WAM).

Sezione 3

Conclusioni

L'hijack della sessione non è un nuovo rischio per la sicurezza dato che risale all'HTTP 1.1. Tuttavia, l'attenzione su questo problema è aumentata di recente e le aziende sono consapevoli della necessità di implementare delle misure in grado di risolverlo.

CA Technologies ha sviluppato una soluzione per gestire l'hijack della sessione che confronta le credenziali valide e i cookie di sessione interni di un utente finale con la device fingerprint utilizzata per l'accesso iniziale dell'utente. Enhanced Session Assurance con DeviceDNA fornisce "autenticazione continua", è disponibile "out-of-the-box" per gli utenti di CA Single Sign-On r12.5[2] ed è l'unico prodotto di questo tipo in grado di evitare l'hijack della sessione.

Sezione 4

Definizioni

Cos'è CA Single Sign-On?

Le soluzioni di gestione dell'accesso flessibili CA Single Sign-On sono altamente scalabili e flessibili e forniscono single sign-on sicuro, autorizzazione basata su policy, auditing e amministrazione per applicazioni web e cloud. CA Federation supporta la federazione delle identità basata su standard per consentire agli utenti di accedere in sicurezza alle applicazioni tra i domini. Contribuisce a rendere sicura, disponibile e accessibile la presenza online, eliminando i limiti organizzativi. CA Access Gateway fornisce un gateway proxy ad alte performance dotato di un modello di distribuzione opzionale nell'ambito della gamma di soluzioni per la gestione dell'accesso flessibile e SSO protetto. L'obiettivo è fornire alle aziende accesso online e single sign-on in completa sicurezza.

Cos'è CA Advanced Authentication?

CA Advanced Authentication è una soluzione flessibile e scalabile che integra sia metodi di autenticazione basati sul rischio, come identificazione del device, geolocalizzazione e attività degli utenti, sia un'ampia serie di credenziali di autenticazione forte e multifattore. Questa soluzione è in grado di consentire all'azienda di creare la procedura di autenticazione adeguata a ogni applicazione o transazione. Può essere fornito come software on-premise o come servizio cloud ed è in grado di proteggere l'accesso alle applicazioni da una vasta gamma di endpoint, inclusi tutti i più diffusi device mobile. Questa soluzione completa è in grado di consentire all'azienda di implementare in modo conveniente il metodo di autenticazione forte adeguato negli ambienti senza gravare sugli utenti finali.

CA Strong Authentication è un server di autenticazione versatile per distribuire e applicare in modo efficiente e centralizzato un numero elevato di solidi metodi di autenticazione. Consente l'interazione online sicura con dipendenti, clienti e cittadini offrendo un'autenticazione forte multifattore per applicazioni interne e basate sul cloud. Comprende applicazioni di autenticazione mobile e SDK, nonché diverse forme di autenticazione out-of-band.

CA Risk Authentication offre all'azienda un'autenticazione multifattore in grado di rilevare e bloccare le frodi in tempo reale, senza interazione con l'utente. Si integra con qualsiasi applicazione online, inclusi siti web/portali e VPN, e analizza il rischio di tentativi di accesso e transazioni online. Questa forma di autenticazione multifattore, invisibile all'utente finale, utilizza fattori contestuali come ID device, geolocalizzazione, indirizzo IP e informazioni sull'attività dell'utente per calcolare un punteggio di rischio e consigliare l'azione opportuna.

DeviceDNA identifica i device che accedono alle applicazioni. Fornisce informazioni riepilogative sulla natura del device, ad esempio tipo di device e ID device univoco, in modo da valutare il livello di rischio.

Sezione 5

Per ulteriori informazioni

Session Linking viene descritto più dettagliatamente nel white paper di CA Technologies intitolato "Session Linking and Session Assurance".

Sezione 6

L'autore

Martin Yam è uno Strategic Advisor presso CA Technologies. Prima di unirsi a CA Technologies, Yam era vicepresidente delle vendite mondiali per Arcot Systems, Inc. Yam ha inoltre ricoperto le posizioni di executive e sales manager presso Oracle, Informix, Accrue Software, ParcPlace Systems e NeXT.

Il sito di CA Technologies è disponibile all'indirizzo ca.com/it

CA Technologies (NASDAQ: CA) crea software che promuove l'innovazione all'interno delle aziende, consentendo loro di sfruttare le opportunità offerte dall'economia delle applicazioni. Il software rappresenta il cuore di qualsiasi business, in ogni settore. Dalla pianificazione allo sviluppo, fino alla gestione e alla sicurezza, CA Technologies lavora con le aziende di tutto il mondo per cambiare il nostro modo di vivere, interagire e comunicare, in ambienti mobili, cloud pubblici e privati, distribuiti e mainframe. Per ulteriori informazioni, visitare il sito **ca.com/it**.

1 L'URL completo è 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 gennaio 2014.

CS87229_0914