WHITE PAPER | DECEMBER 2014

Closing the Biggest Security Hole in Web Application Delivery

Addressing Session Hijacking with CA Single Sign-On Enhanced Session Assurance with DeviceDNA™

Martin Yam
CA Security Management Team

ca technologies

Executive Summary

Challenge

Since the beginning of web application delivery, there has been an opportunity for fraudsters to get into the middle of a transaction and impersonate the legitimate user. Since the credentials used for this fraud are valid and "expected to be under the control of the real user," this type of impersonation has been difficult if not impossible to detect and stop.

Opportunity

The threat of "session hijacking" is an area of growing concern among enterprises with assets to protect, while at the same time providing easy, yet secure access to their users. It is one of the leading security issues facing enterprises today. Many leading experts identify "session hijacking" as a nearly permanent security risk (see Wikipedia.org).

The Open Web Application Security Project (OWASP) highlights this vulnerability in its Top 10 list for 2013[1]. The two categories listed below are specific cases of poor authentication and session hijacking.

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

This points out the high visibility of this problem and makes a solution that can help address it much more valuable.

Benefits

CA Technologies has developed a solution to this security problem that crosses all commercial off-the-shelf (COTS) and homegrown Web Access Management (WAM) solutions by tying the user's valid credentials, and session cookie, to the device fingerprint that was used for the initial user login. Periodically checking this credential/device combination during a transaction session and validating it can ensure that the actual user is continuing their transaction and that their session has not been hijacked.

Section 1

The Importance of "Continuous Authentication"

Session hijacking, also known as cookie hijacking, is not a new threat, having evolved into an almost permanent security risk since HTTP 1.1 became a standard. A recent Forrester Research report discusses 'continuous authentication' which from our perspective recognizes the threat session hijacking poses. Number four in Forrester Research's "OUR PREDICTIONS FOR IAM IN 2014" [2] is:

Continuous authentication will protect sessions start to finish. *Using IP addresses, or device IDs and their reputation, no longer sufficiently protects against threats because these parameters mainly affect only the first step in user interactions: front-door authentication. Once the user is logged in, they offer little protection. Enter continuous authentication: watching user behavior (mainly on the web channel in the first phase and on other channels in later phases) to determine if the user is navigating the site in an orderly manner. If there is cause for alarm — the user's agent is scraping the site at high speeds or there is a suspicion of an attack or data exfiltration — the solution can alert administrators and optionally even terminate the session.*

What you need to do about it. *To protect against suspicious sessions, you have to establish a good behavior baseline. You'll have to ask your risk-based authentication (RBA) solution vendor to see if it can establish a user activity baseline before routine operations begin — because getting this information any other way is almost impossible.*

CA Technologies offers Enhanced Session Assurance with DeviceDNA to provide "continuous authentication" and it is available "out-of-the-box" for users of CA Single Sign-On r12.52. Through another CA Single Sign-On feature called "Session Linking," this capability can also be extended to protect applications that use their own session cookies, like Tivoli Access Manager, Oracle Access Manager or many homegrown solutions. It's important to note that this can be done without any modifications required to these other applications.

Enhanced Session Assurance with DeviceDNA takes advantage of existing CA solution components. It uses the ability contained in CA Risk Authentication to identify and collect machine characteristics of the legitimate user's device from their initial logon sequence and compare this periodically with the actual device being with the session cookie during the user's session. The time between device checks is configurable to improve performance and allow this checking to occur at high value portions of the session.

How the Problem Occurs

Hackers want to exploit the easiest path to break into a system. With the growing adoption of other authentication technologies, it is harder to steal login credentials so fraudsters are finding new and creative ways to get into a valid, authenticated transaction flow. It is expected that this exploit will continue to grow at a faster rate in the future.

Stronger credentials can be used as enterprises try to prevent a hacker from stealing a session cookie. Two-factor credentials delivered as CA Strong Authentication can help build security at the front door, but with single factor credentials such as Active Directory (AD) username/password, the challenge is how good the application security is AFTER the session is stolen. Using network-based information can be helpful, but various networking devices can easily spoof or hide IP addresses.

Enhanced Session Assurance with DeviceDNA/Continuous Authentication from CA Technologies represents a significant step forward in preventing stolen session replay.

By leveraging patent-pending DeviceDNA technology, which is available in CA Risk Authentication, CA Single Sign-On can identify the client and determine if the accessing device has changed in the midst of the session.

On a configurable, periodic basis, CA Single Sign-On will re-check that the current client device is identical to the device that originally logged in to begin the session. If a mismatch occurs, there is a high likelihood that an attacker has hijacked the session. In this case, the application can request that the user re-authenticate using secondary credentials, or it can simply log the user out with a message to restart their session. This feature can be enabled on an application-by-application basis. Different applications can have different re-check rates based on the value of the asset that is being protected or accessed.

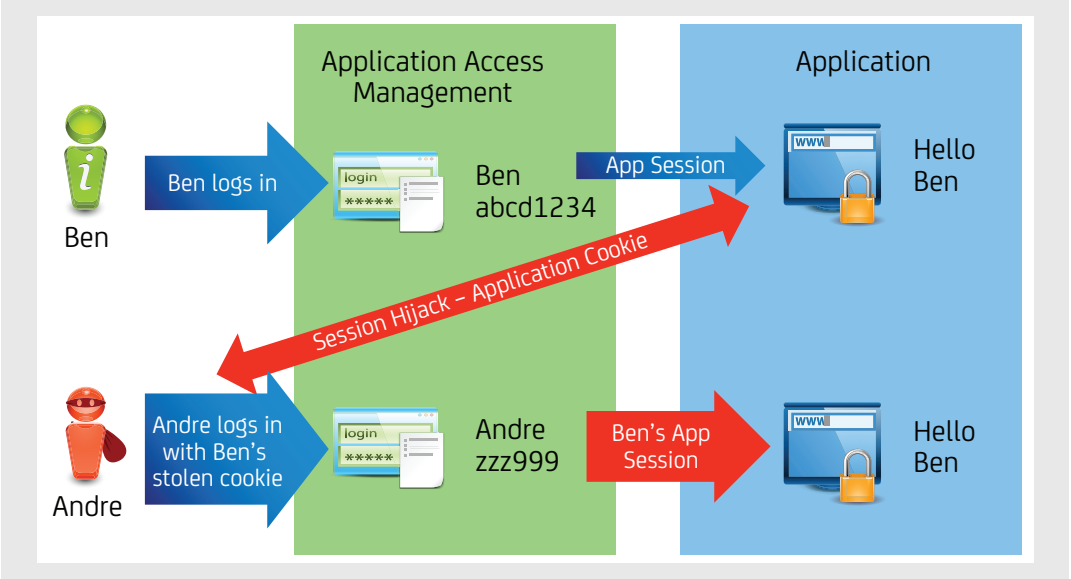
The graphic below describes how session hijacking occurs and the resultant threat to the enterprise application.

Step 1: Ben, the legitimate user, logs in and is authenticated to the application.

Step 2: Andre, the fraudster, steals Ben's session cookie credential.

Step 3: Andre now logs in using Ben's session cookie credential; the application thinks it's Ben, knows that he is a legitimate user and grants him the same access.

Figure A.



Section 2

Extending Continuous Session Assurance into the Application

CA Access Gateway offers another feature that can extend this security for the CA Single Sign-On session down to the application's session as well. The Session Linker feature is designed to examine inbound requests to validate that session cookies from applications are only used in conjunction with the CA Single Sign-On session that they were created for. If the Session Linker detects that a user is presenting an application cookie from a different user, and their own CA Single Sign-On session (to try and get past the session assurance checks), the user is logged out. One can use this Session Linking feature combined with Enhanced Session Assurance with DeviceDNA to secure application cookies or even the tokens of other non-CA Single Sign-On Web Access Management (WAM) solutions.

Section 3

Conclusion

Session hijacking is not a new security risk, having been possible since HTTP 1.1. However, its profile has risen recently and organizations are aware of the need to put measures in place to combat it.

CA Technologies has developed a solution to address session hijacking that compares an end user's valid credentials and internal session cookie to the device fingerprint that was used for the initial user login. Enhanced Session Assurance with DeviceDNA provides "continuous authentication" and it is available "out-of-the-box" for users of CA Single Sign-On r12.52 and is the only product of its kind that can help to prevent session hijacking.

Section 4

Definitions

What is CA Single Sign-On?

CA Single Sign-On flexible access management solutions are highly-scalable, flexible access management solutions that provide secure single sign-on, policy-based authorization, auditing and administration for Web and cloud applications. CA Federation supports standards-based identity federation to allow users to securely access applications across domains. It helps to make your online presence secure, available and accessible—without organizational boundaries getting in the way. And CA Access Gateway delivers a high-performance proxy gateway that provides an optional deployment model in the secure SSO & flexible access management family for securely enabling online business and single sign-on.

What is CA Advanced Authentication?

CA Advanced Authentication is a flexible and scalable solution that incorporates both risk-based authentication methods like device identification, geolocation and user activity, as well as, a wide variety of multi-factor, strong authentication credentials. This solution can allow the organization to create the appropriate authentication process for each application or transaction. It can be delivered as on-premise software or as a cloud service and it can protect application access from a wide range of endpoints including all of the popular mobile devices. This comprehensive solution can enable your organization to cost effectively enforce the appropriate method of strong authentication across environments without burdening end users.

CA Strong Authentication is a versatile authentication server that allows you to deploy and enforce a wide range of strong authentication methods in an efficient and centralized manner. It enables secure online interaction with your employees, customers and citizens by delivering multi-factor strong authentication for both internal and cloud-based applications. It includes mobile authentication applications and SDKs as well as several forms of out-of-band authentication.

CA Risk Authentication offers your organization multi-factor authentication that can detect and block fraud in real-time, without any interaction with the user. It integrates with any online application, including websites/portals and VPNs and analyzes the risk of online access attempts and transactions. This form of multi-factor authentication, which is invisible to the end-user, utilizes contextual factors such as Device ID, geo-location, IP address and user activity information to calculate a risk score and recommend the appropriate action.

DeviceDNA identifies devices that are accessing your applications. Summary information about the nature of the device such as type of device and the unique device ID are provided so that the level of risk can be assessed.

Section 5

For Additional Information

Session Linking is covered in more detail in a companion white paper from CA Technologies entitled “Session Linking and Session Assurance.”

Section 6

About the Author

Martin Yam is a Strategic Advisor at CA Technologies. Prior to joining CA Technologies, Yam was vice president of worldwide sales for Arcot Systems, Inc. Yam has also held executive and sales management positions at Oracle, Informix, Accrue Software, ParcPlace Systems and NeXT.

Connect with CA Technologies at ca.com

CA Technologies (NASDAQ: CA) creates software that fuels transformation for companies and enables them to seize the opportunities of the application economy. Software is at the heart of every business, in every industry. From planning to development to management and security, CA is working with companies worldwide to change the way we live, transact and communicate – across mobile, private and public cloud, distributed and mainframe environments. Learn more at **ca.com**.

1 The full URL is 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., January 7, 2014.

CS87229_0914