WHITE PAPER | 2014 年 12 月

Web アプリケーション・デリバリにおける最大のセキュリティ・ホールの解消

CA Single Sign-On Enhanced Session Assurance with DeviceDNA ™を使用したセッション・ハイジャックへの対応

Martin Yam
CA セキュリティ・マネジメント・チーム

ca technologies

概要

課題

Web アプリケーション・デリバリの開始以来、攻撃者がトランザクションに介入したり正規のユーザになりすますなどの事態が発生しています。このような不正では「正規ユーザの管理下にあると期待される」有効なクレデンシャルが使用されるため、この種のなりすましを検出し阻止することは不可能ではないにしても困難でした。

ビジネス・チャンス

資産を保護しながら簡単かつ安全なアクセス方法をユーザに提供しなければならない企業にとって、「セッション・ハイジャック」の脅威に対する懸念は高まっています。これは現在の企業が直面するセキュリティ上の大きな課題の 1 つです。多くの主要な専門家は、「セッション・ハイジャック」をほぼ永続的なセキュリティ・リスクであるとしています（Wikipedia.org 参照）。

Open Web Application Security Project（OWASP）は 2013 年の上位 10 の脆弱性にセッション・ハイジャックをあげています [1]。不十分な本人認証とセッション・ハイジャックの具体例として以下の 2 つのカテゴリがあります。

1. A2 – 不十分な認証とセッション管理
2. A3 – クロスサイト・スクリプティング（XSS）

つまりこの問題への注目度は高く、これに対応できるソリューションは価値が高いということです。

メリット

CA Technologies はユーザの有効なクレデンシャルとセッション・クッキーを初期ユーザ・ログインに使用されたデバイスのフィンガープリントに関連付けることで、あらゆる市販（COTS）および自前の Web アクセス・マネジメント（WAM）ソリューションにまたがってこのセキュリティ問題に対応できるソリューションを開発しました。トランザクションのセッション中にこのクレデンシャルとデバイスの組み合わせを定期的に確認し検証することで、実際のユーザがトランザクションを続行しており、そのセッションがハイジャックされていないことを確認できます。

セクション 1

「継続的な本人認証」の重要性

クッキー・ハイジャックとも呼ばれるセッション・ハイジャックは新しい脅威ではなく、HTTP 1.1 が標準になって以降ほぼ継続的なセキュリティ・リスクになりました。最近の Forrester Research レポートでは「継続的な本人認証」について取り上げられていますが、CA の観点からするとこれはセッション・ハイジャックが引き起こす脅威が認められたということです。Forrester Research による「OUR PREDICTIONS FOR IAM IN 2014（2014 年の IAM 予測）」[2] の第 1 項には以下のように記載されています。

継続的な本人認証によってセッションを始めから終わりまで保護されます。 IP アドレスやデバイス ID はその信頼性の評価が高くても、主としてユーザ・インタラクションの最初の段階である入口の本人認証にしか関与しないため、現在では脅威に対して十分な保護を提供できなくなっています。一度ユーザがログインしてしまえば、防御の機能はほとんど果たしません。継続的に本人認証を行って、ユーザの動作を監視すれば（最初の段階では主に Web チャネル上、その後は他のチャネル上で）、ユーザが規則に従ってサイトを利用しているか判断できます。警戒すべき要因が発生した場合、たとえばユーザのエージェントが高速でサイトを破壊していたり、攻撃やデータの引き出しの疑いがある場合、ソリューションが管理者にアラートを送信し、状況によってはセッションを終了させることも可能です。

そのためには何をすればいいでしょうか。 疑わしいセッションに対して防御するには、望ましい動作の基準を確立する必要があります。日常的な運用を始める前に、ユーザ・アクティビティの基準を確立することが可能かどうか、リスクベースの本人認証（RBA）ソリューションのベンダに尋ねて確認する必要があります。この情報は他の方法ではほとんど得ることができません。

CA Technologies の Enhanced Session Assurance with DeviceDNA は「継続的な本人認証」を提供します。これは CA Single Sign-On r12.52 のユーザであれば導入後すぐに使用できます。この機能は CA Single Sign-On の別の機能である「セッション･リンカー」を使用すれば、Tivoli Access Manager や Oracle Access Manager、あるいは多くの自前のソリューションなど独自のセッション・クッキーを使用するアプリケーションを保護するよう拡張することもできます。
これら他のアプリケーションに変更なしで対応できることは、特筆すべき点です。

Enhanced Session Assurance with DeviceDNA は CA ソリューションの既存のコンポーネントを活用します。CA Risk Authentication に含まれる機能を使用し、正規ユーザの初期ログオン・シーケンスからユーザ・デバイスのマシン特性を識別・収集して、ユーザ・セッション中この情報を定期的に、セッション・クッキーと共に使用される実際のデバイスと比較します。デバイスのチェックを行ってから次のチェックまでの間隔はパフォーマンスを向上させるために変更可能で、セッションの価値の高い部分でチェックを行うよう設定することができます。

問題が起きる過程

ハッカーは一番簡単なパスを利用してシステムに侵入しようとします。他の本人認証テクノロジの導入が増えたことでログイン･クレデンシャルの盗用が以前より難しくなったため、攻撃者は有効な認証済みのトランザクション・フローに侵入すべく新しい独創的な方法を探しています。このような侵入手段は今後もっと速い速度で増え続けることが予測されています。

ハッカーによるセッション・クッキー盗用を防止する方法としては、より強力なクレデンシャルの使用があります。CA Strong Authentication などの二要素クレデンシャルなら入口のセキュリティは確保できます。しかし、Active Directory（AD）のユーザ名 / パスワードなどの単一要素のクレデンシャルの場合は、セッションが盗まれた後にアプリケーションのセキュリティがどれだけ有効であるかが問題になります。ネットワークベースの情報の使用は役に立ちますが、さまざまなネットワーク・デバイスが IP アドレスを簡単に偽ったり隠蔽することができます。

CA Technologies の Enhanced Session Assurance with DeviceDNA による継続的な本人認証は、盗まれたセッションのリプレイ攻撃を防止する上で大きな進歩です。

CA Risk Authentication で利用可能な特許申請中の DeviceDNA テクノロジを活用することで、CA Single Sign-On はクライアントを識別でき、アクセス先のデバイスがセッションの途中で変わっていないか判断できます。

CA Single Sign-On では、設定した周期で現在のクライアント・デバイスがセッション開始時に最初にログインしたデバイスと同じものであることを再確認できます。これが一致しない場合はセッションがハイジャックされた可能性が高くなります。その場合、アプリケーションは 2 番目のクレデンシャルを使用してユーザに再認証を求めることができるほか、セッションを再び開始するようメッセージを表示してユーザをログアウトさせることも可能です。この機能はアプリケーションごとに有効にできます。保護あるいはアクセスの対象となる資産の価値に基づき、アプリケーションごとに再確認の度合いを変えることもできます。

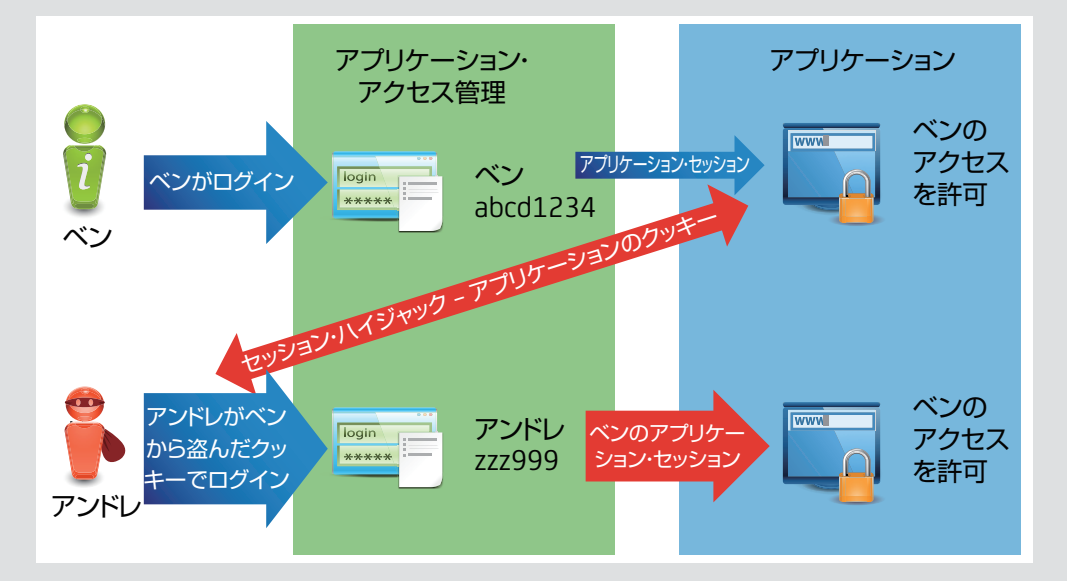
次の図は、セッション・ハイジャックが起きる過程と、それによる企業のアプリケーションへの脅威を示しています。

手順 1: 正規のユーザであるベンがログインし、アプリケーションへのアクセスが認証されます。

手順 2: ハッカーのアンドレは、ベンのセッション・クッキー・クレデンシャルを盗みます。

手順 3: アンドレはベンのセッション・クッキー・クレデンシャルを使用してログインします。アプリケーションはそれをベンとみなし、ベンは正規ユーザであるため同じアクセスが許可されます。

図 A



セクション 2

継続的なセッション保証をアプリケーションに拡張

CA Access Gateway では、CA Single Sign-On セッション向けのこのセキュリティをアプリケーションのセッションに拡張することができます。セッション・リンカー機能はインバウンドのリクエストを調査し、アプリケーションのセッション・クッキーがその生成目的である CA Single Sign-On のセッションと併用してのみ使用されていることを確認します。ユーザが別のユーザのアプリケーション・クッキーと自身の CA Single Sign-On セッションを使用している（セッション保証チェックをかわすため）のをセッション･リンカーが検出すると、そのユーザはログアウトさせられます。このセッション・リンカー機能は Enhanced Session Assurance with DeviceDNA と組み合わせて使用でき、アプリケーション・クッキーや CA Single Sign-On Web アクセス・マネジメント（WAM）ソリューション以外の他のトークンも保護することができます。

セクション 3

まとめ

セッション・ハイジャックはセキュリティ上の新しいリスクではなく、HTTP 1.1 以来存在していた脅威です。しかし、近年その件数が目立つようになり、それに対抗するための措置を取る必要があることが認識されるようになりました。

CA Technologies が開発したソリューションは、エンドユーザの有効なクレデンシャルと内部セッション・クッキーを、初期ユーザ・ログインに使用されたデバイス・フィンガープリントと比較してセッション・ハイジャックに対抗します。Enhanced Session Assurance with DeviceDNA の「継続的な本人認証」は、CA Single Sign-On r12.52 のユーザであれば導入後すぐに使用でき、セッション・ハイジャックの防止に役立つ唯一の製品です。

セクション 4

定義

CA Single Sign-On について

CA Single Sign-On アクセス・マネジメント・ソリューションは拡張性と柔軟に優れ、Web およびクラウド・アプリケーションに安全なシングル・サインオン、ポリシーベースの権限認証、監査、管理を提供します。CA Federation は標準ベースのアイデンティティ・フェデレーションをサポートしているため、ユーザはドメイン間にまたがるアプリケーションに安全にアクセスできます。また、組織の境界に邪魔されることなく、オンライン・プレゼンスのセキュリティ、可用性、アクセシビリティを確保できます。CA Access Gateway のパフォーマンスに優れたプロキシ・ゲートウェイは、オンライン・ビジネスとシングル・サインオンの安全性を確保するため、安全な SSO および柔軟なアクセス・マネジメント・ファミリのオプション導入モデルを提供します。

CA Advanced Authentication について

CA Advanced Authentication は、デバイスの識別、位置情報、ユーザ・アクティビティなどのリスクベースの本人認証方式と、多様なマルチファクタによる強力な認証クレデンシャルを組み合わせた柔軟かつ拡張可能なソリューションです。
このソリューションを利用することで、組織はアプリケーションまたはトランザクションごとに適切な本人認証プロセスを構築できます。このソリューションはオンプレミスのソフトウェアあるいはクラウド・サービスとして導入でき、人気のあるモバイル・デバイスのすべてを含む、さまざまなデバイスからのアプリケーションへのアクセスを保護できます。この包括的なソリューションは、エンドユーザに負担をかけることなく、環境全体にわたって強力な本人認証を適切な方式でコスト効率良く徹底できるようになります。

CA Strong Authentication は、さまざまな認証方法を効率的かつ一元的に導入することを可能にする万能の認証サーバです。マルチファクタの強力な本人認証のクレデンシャルを内部アプリケーションとクラウドベース・アプリケーションの両方に提供することで、社員、顧客、一般ユーザとの安全なオンライン・インタラクションを促進します。これにはモバイル認証アプリケーション、SDK、および複数の形式の帯域外の認証が含まれます。

CA Risk Authentication は、ユーザの操作を介さずに不正をリアルタイムで検出するマルチファクタの本人認証を提供します。Web サイト / ポータルや VPN などのオンライン・アプリケーションを統合し、オンライン・アクセス試行とトランザクションのリスクを分析します。エンドユーザには見えないこの形式のマルチファクタ本人認証はデバイス ID、位置情報、IP アドレス、ユーザ・アクティビティ情報などのコンテキスト要因を使用してリスク・スコアを計算し、適切なアクションを推奨します。

DeviceDNA はアプリケーションにアクセスしているデバイスを識別します。デバイスの種類や一意のデバイス ID などデバイスの性質に関するサマリ情報を提供し、リスク・レベルの評価を可能にします。

セクション 5

その他の情報

セッション・リンカーの詳細については、CA Technologies のホワイトペーパー「Session Linking and Session Assurance（セッション・リンカーとセッション保証）」で説明しています。

セクション 6

著者について

Martin Yam は CA Technologies の戦略アドバイザーです。CA Technologies 入社以前は、Arcot Systems, Inc. の国際営業担当バイス・プレジデントを務め、また、Oracle、Informix、Accrue Software、ParcPlace Systems、NeXT でもエグゼクティブや営業管理の経験があります。

ca.com/jp/でCA Technologiesにアクセスしてください

CA Technologies（NASDAQ:CA）は、企業の変革を推進するソフトウェアを開発し、アプリケーション・エコノミーにおいて企業がビジネス・チャンスを獲得できるよう支援します。ソフトウェアはあらゆる業界であらゆるビジネスの中核を担っています。プランニングから開発、管理、セキュリティまで、CA は世界中の企業と協力し、モバイル、プライベート・クラウドやパブリック・クラウド、分散環境、メインフレーム環境にわたって、人々の生活やビジネス、コミュニケーションの方法に変化をもたらしています。詳細については **ca.com/jp** をご覧ください。

1 URLは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（2014年の予測: アイデンティティ/アクセス・マネジメント、社員と顧客のIAMがクラウドへ）」、Forrester Research, Inc.、2014年1月7日