WHITE PAPER | 2014 年 8 月

パスワードの送信と保存が不要なセキュリティ侵害対策

ca technologies

目次

次の被害者として報道されないために

ニュースでは毎日、新しいセキュリティ侵害が報じられています。実際、ニューヨーク・タイムズ紙によって最近、数十億のオンライン・アカウントのパスワードがセキュリティ侵害によって漏洩したと報じられました。なぜこのようなことが次々と起こるのでしょうか。その理由の 1 つは、いまだに多くの Web サイトが認証に単純なパスワードを使用し、ハッシュとして保存しているからです。もう 1 つの理由は、アイデンティティの盗用や詐欺は大金を稼げるビジネスだからです。

Ponemon Study によると、米国企業はデータ侵害で平均総額 540 万ドルを超える最高の被害を記録しました。この調査によると、このような被害をもたらした原因に、米国企業がデータを侵害された結果、漏洩したデータとウイルスに感染したデータが最も多かったことが挙げられます。これは、実際の被害金額ですが、ブランドや顧客の信頼への影響を考えればそのコストはビジネスにとってさらに大きなものとなります。

「侵害できるセキュリティ」から侵害できないセキュリティへ

ハッカーがクレデンシャルのデータベースを入手して、ハッシュや暗号化を使用したパスワードが保存されていないことを知ったらどうなるでしょう。CA Advanced Authentication の導入により、パスワード盗難の問題を解決できます。強力な認証クレデンシャルによってパスワードのハッシュ・ファイルが不要になるため、セキュリティ侵害を防止できます。つまり、「侵害できるセキュリティ」を侵害できないセキュリティにすることができるのです。

パスワードが攻撃されやすい理由

セキュリティ侵害の攻撃の対象になりやすいのは、パスワードのリポジトリ、たとえば、パスワードのハッシュ・ファイルです。一般的なパスワードの保護では、ハッシュのアルゴリズムが使用されます。ただし、それらを保存するデータベースはハッカーの格好の標的であり、「総当たり攻撃」でパスワードを盗まれてしまいます。既存の大抵の総当たり攻撃で、それほど時間をかけずにこれらのファイルを解読できます。認証に単純なパスワードを使い続けることやハッシュの保存が（通常、「salt」を追加して保護を強化）、このような攻撃を可能するのです。

ハッシュ化とは、パスワードなどの 1 つのデータを無作為のデータ、またはそれと認識できない別のデータに変換することを意味します。たとえば、「MiloPug」というパスワードをハッシュ化すると、**「xh^21hdgXEOUD76@%@d」**になります。また、ハッシュ化は一方通行です。元のテキストからハッシュを作成するのは簡単ですが、ハッシュから元のテキストに戻すことはできません。ハッシュ関数を元に戻すアルゴリズムがないため、総当たりの手法で攻撃するのです。現在の高度なハッキングの手法を考えると、これはあまりむずかしいことではありません。

パスワードの保存が不要なセキュリティ侵害対策

コンセプト自体は簡単です。現在、多くのシステムでは、ユーザの入力したパスワードのハッシュをサーバに保存したハッシュ値と比較して認証しています。CA Technologies が採用した新しいアプローチでは、パスワードはもちろん、ハッシュでさえも保存する必要はありません。特許取得の「暗号化カモフラージュ」（米国特許 6,170,058）を使用して、CA Advanced Authentication によってパスワードで秘密鍵が保護または「ロック」されます。保護された鍵はサーバからブラウザまたはアプリケーションに送信され、そこでパスワードを使用してロックが解除されます。ロック解除された鍵はその後、ランダムチャレンジの入力に使用され、その入力がサーバに返信されます。そのパスワードとロック解除された鍵によってブラウザのメモリが使用されるのは、ほんのわずかな時間だけです。

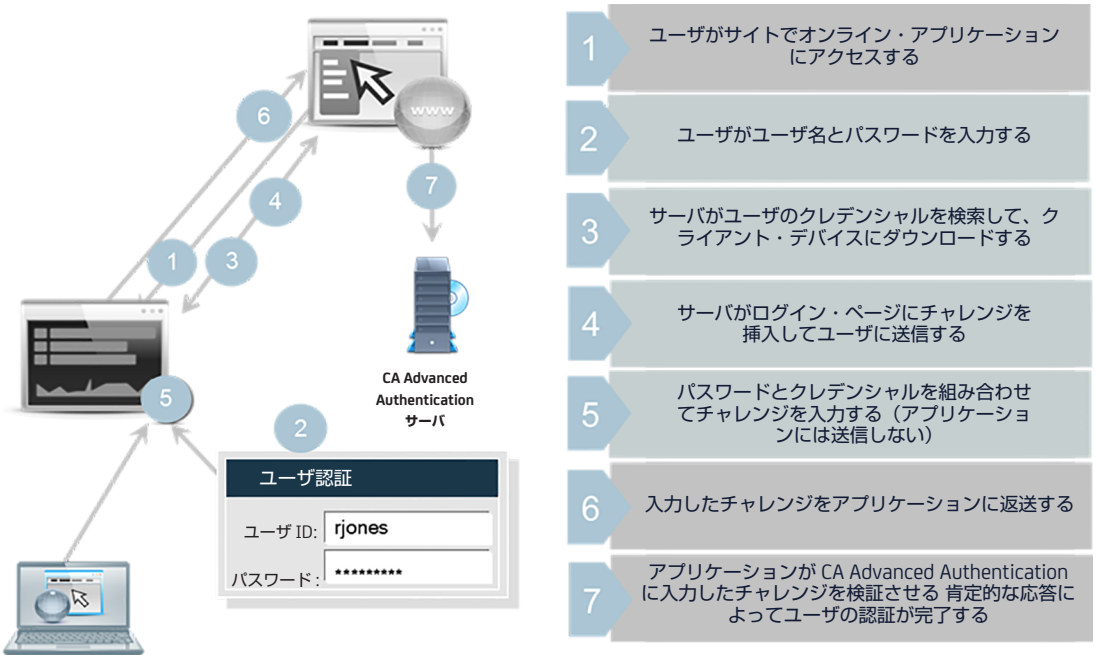
カモフラージュ・テクノロジでは、攻撃者が保護された鍵を入手してもロック解除できません。パスワードはユーザの頭の中だけに記憶され、攻撃者が盗むパスワード・ファイルは存在しません。パスワードはクレデンシャルの作成と認証プロセスに使用されますが、どこにも保存されません。リポジトリにも保存されません。クライアントにも保存されません。ハッカーが標的にできるような場所には一切保存されないのです。

CA Advanced Authentication の機能

登録プロセスでは、エンドユーザが CA Auth ID を設定すると、PIN またはパスワードを選択するようメッセージが表示され、各エンドユーザには秘密鍵と公開鍵の鍵ペアが割り当てられます。CA の特許取得の暗号化カモフラージュ・テクノロジを使用して、秘密鍵はユーザの PIN またはパスワードをベースにカモフラージュされます。カモフラージュは、総当たり攻撃を防止する標準の暗号化アルゴリズムをベースにしたデータ保護の手法です。この手法では、誤ったパスワードを使用していても復号化すると必ず結果が表示されますが、攻撃者には正しいパスワードのように見えても有効なシグネチャは作成されません。そのシグネチャが返送されると、サーバによって検出されます。

単純な 6 桁のパスワード（文字、数字、10 個の特殊文字を使用）の場合、カモフラージュされた鍵への総当たり攻撃によって「726 = 139,314,069,504」という本物のように見える鍵が作成されます。これらのうち 1 つだけ有効なシグネチャが作成されますが、攻撃者にはそれがどれだかわかりません。これらはすべて有効に見えます。攻撃者はシグネチャをサーバに送信して、つまり、認証を試行して、これらの鍵を 1 つずつ試すほかに方法がありません。何度か失敗すると、サーバによって攻撃が検出されます。

以下の図は、サーバにパスワードを送信せず、パスワード・リポジトリに対して検証する必要のない CA Advanced Authentication のパスワードの使用を示しています。



問題を解決するテクノロジ

CA Auth ID のクレデンシャルは誰でも、攻撃者であってもユーザ名を使用して利用できます。ただし、総当たり攻撃できないため、残念ながら攻撃には利用できません。ID はログイン時にサーバから提供されるため、デバイスや場所を問いません。JavaScript® をインストールし、ソフトウェア開発ツールキット（SDK）を使用して開発したモバイル・アプリケーションに対応したデバイスなら、どのデバイスでも使用できます。

既存の登録プロセスや「パスワードを忘れましたか ?」（FYP）など、他のパスワードのプロセスとの違いをユーザが認識することはありません。既存のリスクや二次認証のプロセスは維持されます。ログインのフローと既存のログインの順番（シングル・ページまたはダブル・ページ）も変更されません。ユーザは現在のクレデンシャルの「裏側」から、「同一に見える保護された」クレデンシャルに移動します。

CA AuthID は二要素認証のコンプライアンス要件の遵守にも使用できますが、その場合は、実績あるクレデンシャルを使用するため、パスワード・データベースを作成、管理および保護する必要はありません。そのため、ハッカーの最も魅力的な標的である、総当たり攻撃に脆弱で大規模なクレデンシャル・リポジトリが不要になります。

CA Advanced Authentication には、以下のメリットがあります。

- サーバ側のハッシュ・ファイルへの攻撃の防止
- パスワード転送時を狙った中間者攻撃からの保護
- 使い慣れたユーザ名 / パスワードによるログイン・プロセス
- 複雑なパスワードと保存が不要
- 多様なリスクベースのソリューションに対応
- あらゆるブラウザとデバイスに対応、クライアント側のディスク領域が不要、モバイル・アプリケーション向けの単純な SDK

まとめ

CA Advanced Authentication 製品スイートを使用すれば、セキュリティ侵害で組織の名前が報道されることはありません。このソリューションは既存のアプリケーションと簡単に統合でき、多くのシステムの弱点であるパスワード・ハッシュ・ファイルが不要になります。CA Advanced Authentication で提供される「パスワードのような」クレデンシャルではパスワードがサーバに保存されないため、攻撃者にセキュリティを侵害されて、パスワードを盗まれることもありません。

追加情報：

- 「Be Smarter Than a Hacker」のウェブキャスト（http://bit.ly/1s38Ygj）
- 「The eduCAte Channel for CA Advanced Authentication」（http://bit.ly/1xErzQh）

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 「Cost of a Data Breach Study:Global Analysis」Ponemon Institute、2013 年 5 月

CS200-200-86850_0814