Swivel の二要素認証

概要

本ホワイトペーパーでは、従来型のユーザー名とパスワードの組合せによる認証方式がなぜ脆弱なのかを考察し、Swivel Secure の二要素認証プラットフォームが強力なセキュリティを低コストで提供できる理由、そして利用も管理もどれだけ簡単かをご説明します。

SecurityStrings

SWIVEL
the power of knowing

はじめに

モバイル機器からのリモートアクセスや Web ベースの商取引の急速な普及と共に、便利でコスト対効果が高く、強力なセキュリティを提供できる認証モデルの必要性が高まっています。これまで一般的だった単一要素 (ユーザー名とパスワード) に頼る認証モデルは、多くのアプリケーションにとって、もはや適切な認証方法とは言えなくなっています。

そのため、多要素認証が注目されています。多要素認証は、「知っていること」(パスワードなど) と「持っていること」(何らかの形態の認証トークンなど) という複数の要素を使って認証を行う方法です。

二要素認証に対する Swivel のアプローチの特徴は、ユーザーが特定の認証トークンを必要としないことです。これに、特許取得済みのワンタイムパスワード抽出プロトコルである PINsafe を組み合わせることにより、Swivel は強力でコスト対効果が高く、さらに利用も管理も簡単な認証ソリューションを提供できます。

単一要素認証 (Single-Factor Authentication)

ユーザー認証にあたっては、ユーザー自身が正規のユーザーであることを証明しなければなりません。証明のためには以下の様なものを使います :

- 自分しか知らないこと (パスワードなど)
- 自分しか持っていないもの (トークンなど)
- 自分の一部 (指紋、網膜スキャン)

これらを認証のための要素と言います。

初期の認証システム (そして現在でも多くのシステムがその当時のままです) では、認証は単一の要素によって行われていました。ユーザー名とパスワードの組合せです。(UNP: User Name and Password) しかしこの方法は、多くのシステムにおいて適切では無いという認識が広がっています。この事実は、多くの企業が多要素認証に移行していることだけではなく、多くの規制や法律が多要素認証を必須の要件としていることからも明らかです。

こういった動きの背後には、3 つの大きな流れがあります。まず第 1 に、認証システムによって守るべきシステムの価値が上がっていること、第 2 に、単純な UNP 認証よりも効果を上げることのできるツールが豊富に出回ってきたこと、第 3 にサイバー犯罪の急増です。

ユーザー名とパスワードを狙う攻撃

UNP の弱点のひとつに、パスワードが静的であることが挙げられます。静的とは、いったん設定したパスワードを毎回使うと言うことです。多くの IT 管理者はパスワードを 3 ヶ月毎、あるいは毎月変更するよう呼びかけているでしょうが、それでもハッカーにとって動かない標的を狙うには十分な時間です。

その他の問題としては、IT 管理者やセキュリティ管理者は推測しにくいパスワードを設定することを求めていますが、エンドユーザーやヘルプデスクの管理者は覚えやすいパスワードを望んでいることです。これらは互いに背反します。無作為に並べられた文字列よりは意味のある単語の方が覚えやすいですが、単語は類推されやすいのです。

複雑なパスワードを設定するようユーザーに強制したとしても、こんどは同じパスワードを他のアプリケーションやインターフェースに使い回そうとするでしょう。

認証モデルとしての UNP の最後の弱点は、ユーザー名とパスワードはあまりにも長い間一緒に使われてきた、ということです。今ではソフトウェアベースの攻撃が広く存在しており、それにはインターネットも一役買っています。

ユーザー名とパスワードを狙う攻撃とはどのようなものでしょうか ? 次頁のリストは全てを網羅しようとしたものでは無く、クライアントへの攻撃にフォーカスしたリストです。サーバーへの攻撃やソーシャルエンジアリングをベースにした攻撃 (con-tricks や blackmail など) は含んでいません。

マルウェア攻撃

狙ったコンピュータに悪意を持ったプログラム (マルウェア) を侵入させようとする攻撃です。例えばユーザーのキー入力を監視して記録するキーロガーのようなマルウェアは、どのキーが押されたかを監視することで、入力されたパスワードを特定することができます。その後、ユーザー名とパスワードを記録したログを探します。いくつかのソフトウェア攻撃はもっと洗練されており、ユーザーが特定の行動を起こしたときにキー入力の監視を始めるものもあります。例えば、ユーザーが銀行のサイトにアクセスしたときなどです。パスワードが静的で変化しない場合、こういった攻撃が非常に有効です。

パスワードの類推

パスワードを類推する攻撃には、攻撃者が標的についての情報をどれだけ持っているかによって様々なバリエーションがあります。最も極端な例としては、ブルートフォース攻撃 (総当たり攻撃) があります。侵入に成功するまで、あらゆる文字列の組み合わせを試してみるものです。効率的とは言えませんが、暗号化されたパスワードファイルにアクセスするために使われます。

もう少し範囲を絞った方法として、辞書を使ったものがあります。意味の無い文字列では無く、辞書に載っているような単語や熟語を試してみるもので、多くの人がそういった単語や熟語をパスワードに設定していることから、有効な攻撃です。最後に、攻撃者が標的の個人情報をある程度知っている場合には、好みのスポーツチームや子供の名前を試してみます。これも覚えやすいパスワードを付ける際に多くの人が使う方法です。

パスワードを盗む

複雑なパスワードを望む IT 管理者を満足させるためにユーザーがとる行動の一つとして、そのパスワードを忘れないようにどこかにメモしておく、というものがあります。封筒に書き留めて机の引き出しに入れておくなどです。これを盗むためには物理的にその場に行かなければならないため、攻撃者にとってはハードルが高いですが、このように暗号化もせずにパスワードを書き留めておくというのは驚くほどよく行われていることです。

ショルダーサーフィン (肩越しの覗き見)

誰かのパスワードを知りたければ、それを打ち込んでいるところを盗み見るというのもひとつの方法です。この手口も物理的なアクセスが必要ですが、パスワードが静的であれば、いろいろなチャンスが考えられ、最後には全てを知ることができるでしょう。この手口は「Chip and PIN」(カード決済時に見えないように PIN を入力する) が普及すると共に一般に認知されるようになりました。

フィッシング

フィッシング攻撃に対抗するのは非常に難しいことです。それは、この攻撃を行うのが非常に簡単であることも理由の一つです。企業の正規の Web サイトからイメージやテキストをコピーしてくるのは簡単で、それを使って偽のサイトを作り、どこからか入手したメールアドレスのリストにメールを一斉に配信するだけで良いのです。ユーザーが偽のサイトにアクセスし、ユーザー名とパスワードを入力した瞬間に、攻撃者は欲していたものを手に入れるのです。

二要素認証

認証プロセスにもう一つの要素を加えることは、攻撃者からすれば、ハードルがもうひとつ増えることになります。トークンを使った認証システムの基本的なモデルは、ユーザーにワンタイムパスワードを提供し、それを入力しないと認証されないようにすることです。ワンタイムパスワードは認証の度に変化します。単一要素 (ユーザー名とパスワード) を入手するためには様々な有効な方法があることを見てきました。二要素認証を突破するためには攻撃者は追加で何をする必要があるのでしょう？

二要素認証への攻撃

二要素認証を突破するための攻撃としては、以下の 2 つの方法が考えられます。

トークンを盗む

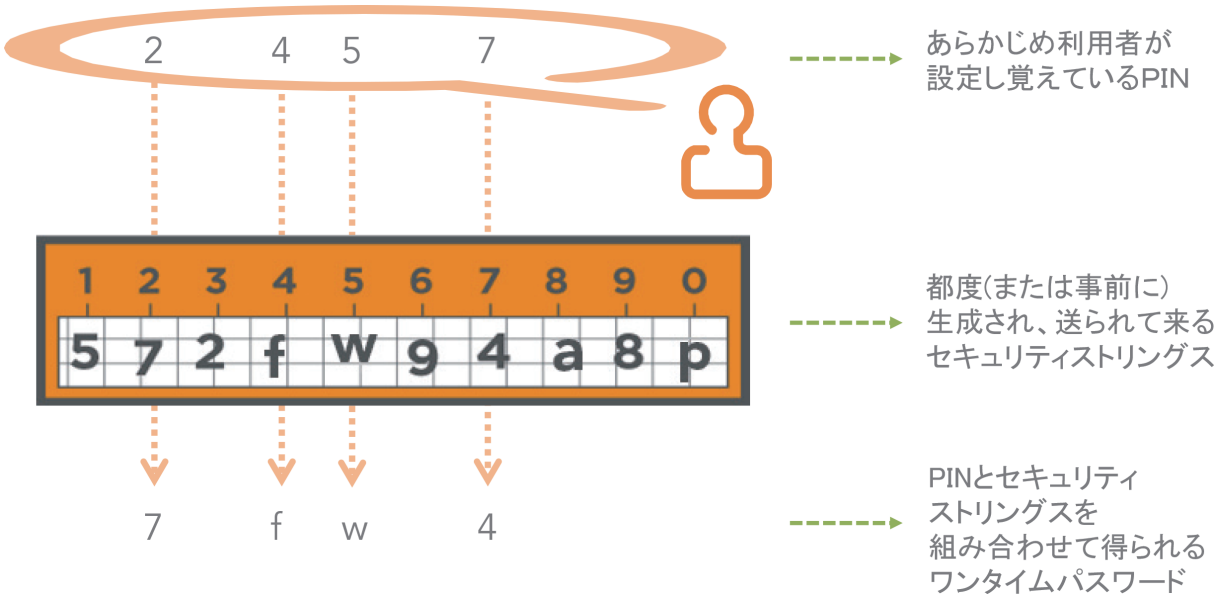
攻撃を成功させるためには、パスワードを盗むソフトウェア攻撃とトークンを物理的に盗み出すことが必要です。パスワードを盗むのは簡単でも、トークンを盗むのは難しいでしょう。しかし、今やたくさんのトークンが配布されていますから、何らかの脆弱性が隠れている可能性もあります。それに攻撃者は、ユーザーがパスワードを入れた同じ引き出しで、たまたまトークンも見つけるかもしれないのです！

フィッシング

フィッシングは二要素認証への攻撃にも有効である可能性があります。攻撃者がユーザーのパスワードとワンタイムパスワードを同時に入手すれば、ユーザーになりすまして認証を突破することが可能だからです。ただ、単一認証でのフィッシングとは違い、二要素認証の場合にはユーザーの手元にトークンがありますから、ログイン情報全てが盗まれたわけではありません。そのため、次の認証を突破するために、攻撃者はもう一度ワンタイムパスワードをフィッシングによって入手しなければなりません。このことから、何度も認証を要求するような Web アプリケーションはフィッシングに対して効果があると言えます。例えば、オンラインバンキングのサイトで、実際の入出金の度に認証を要求するような方法です。

Swivel と二要素認証

Swivel の認証プラットフォームは二要素認証ソリューションですが、他のソリューションとは重要な違いがあります。多くの二要素認証システムと同様に、Swivel もまた、ユーザーの認証に必要な「秘密の文字列」を使います。しかし、文字列は SMS やモバイルアプリを通じて携帯電話などに送られるため、専用のセキュリティトークンを用意する必要がありません。さらに、ユーザーは秘密の文字列そのものを入力するわけではありません。



この文字列をあらかじめ決めてある PIN と組み合わせて、認証のためのワンタイムパスワードを導き出すのです。Swivel ではこれをセキュリティストリングスと呼んでいます。

この方式が何故優れているのかについて、以下にご説明します。

トークンが必要無い

Swivel が専用のセキュリティトークンを使わず、携帯電話などをトークンとして利用することにはいくつものメリットがあります。

まず、物理的に配布するものがありません。ユーザーを登録するために郵便などを使う必要は無く、簡単かつ迅速に登録できます。

これはまた、ユーザーがシステムにアクセスする必要が無くなったときにトークンを回収しなくても良いことを示しています。ユーザーの入れ替わりの激しい教育機関などでの利用においては大きなメリットとなります。

何も言わなくとも、ユーザーは携帯電話を大切に扱います。ビジネスに利用するだけで無く、友人や家族との連絡にも使うからです。携帯電話をどこかに置き忘れたり、服のポケットに入れたまま洗濯に出してしまうようなことは少ないでしょう。また、紛失したり盗まれたりしたときにはすぐに気づくに違いありません。

誰もが持っているデバイスをトークンとして使うということは、認証システムの導入にあたって追加のコストが必要ないと言うことでもあります。

ワンタイムパスワードの抽出

Swivel のワンタイムパスワード抽出プロトコルを使うと言うことは、認証のための二つの要素を一つに組み合わせることを意味しています。これが意味することは :

- ユーザーが認証のために必要とするのは 4 桁のワンタイムパスワードだけです。(Swivel は 4 桁から 10 桁の PIN をパスワードに応じて設定できます)
- PIN そのものが入力されることは絶対にありませんから、前項で説明したキーロガーのような攻撃で盗み取ることは不可能です。

Swivel の二要素認証ソリューションを使えば、先に述べた攻撃のうちのいくつかは非常に難しくなります。物理的なトークンでは無く携帯電話であれば、紛失などの際にもすぐに気づくことができます。攻撃により携帯電話にアクセスされたとしても、それがすぐにセキュリティ上の侵害とはなりません。PIN はキーロガーなどの攻撃では入手することはできず、PIN が無ければ侵入は不可能だからです。

Swivel への攻撃

トークンの盗難

トークンを盗み出したとしても、PIN を入手したことにはなりません。PIN そのものが入力されることは絶対に無いため、キー入力を監視しても PIN を盗み出すことはできないからです。

フィッシング

残念ながら、どのような認証製品も攻撃に対して完全な防御はできません。Swivel に対しても、いくつかの形態のフィッシング攻撃は効果を持つでしょう。先にも述べたように、ユーザーが偽の Web サイトでパスワードを入力してしまうのを止めるのは非常に困難だからです。いったん入力してしまうと、そのパスワードは攻撃者によって再利用されてしまいます。前にも述べたように、その場合でもアカウントがすぐに乗っ取られてしまうわけではありません。携帯電話が無ければ再認証ができないからです。

偽の Web サイトは偽のセキュリティストリングスを送ることにより、ユーザーが入力したワンタイムパスワードから PIN を割り出すことができます。しかしそのためには、攻撃者はユーザーの携帯電話の番号を知っている必要がありますし、SMS を送る方法も必要です。PIN を盗み出したとしても、携帯電話そのものが無ければ使うことはできません。

結論

二要素認証は単一要素認証に比べてはるかに強力な認証システムです。

そして Swivel の二要素認証の実装は、携帯電話をセキュリティトークンとして利用することと、独自のワンタイムパスワード抽出プロトコルを使うことにより、認証の強化と運用コストの削減というメリットがあるのです。

Security Strings 合同会社
〒 102-0082 東京都千代田区一番町 6 番地 相模屋本社ビル 7F
http://www.securitystrings.com/

SecurityStrings