Swivel の多要素認証ソリューション

概要

Swivel は柔軟な認証ソリューションで、幅広い認証モデルをサポートしています。Swivel の特許取得済み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、様々な単一要素または二要素認証ソリューションをご利用頂けます。

はじめに

本ホワイトペーパーでは、Swivel の多要素認証ソリューションの概念と技術についてご説明します。まず、多要素・マルチチャネル認証の概念とメリットについて解説し、Swivel がどのようにしてそれらのアプローチを実現しているかをご説明します。

Swivel 概要

Swivel は多要素認証システムで、チャレンジ - レスポンス型の認証エンジンを中核としています。このエンジンはユーザーにチャレンジを送り、レスポンスをチェックしてそれが正しければアクセスを許可します。

PINsafe

Swivel ソリューションのユニークな特徴として「PINsafe」ワンタイムパスワード抽出プロトコルがあります。PINsafe が発行する「セキュリティストリングス」をユーザーが受けとり、あらかじめ設定してある PIN と組み合わせてワンタイムパスワードを生成し、それを使って認証を行います。

このシステムのメリットは、認証のためにはセキュリティストリングスと PIN が必要になるにもかかわらず、PIN 自体は認証プロセスの中で入力されることは絶対に無いことです。この抽出プロトコルの使い方は簡単で、ワンタイムパスワードのどのキャラクタをどういった順番で使うかを PIN によって決めるのです。

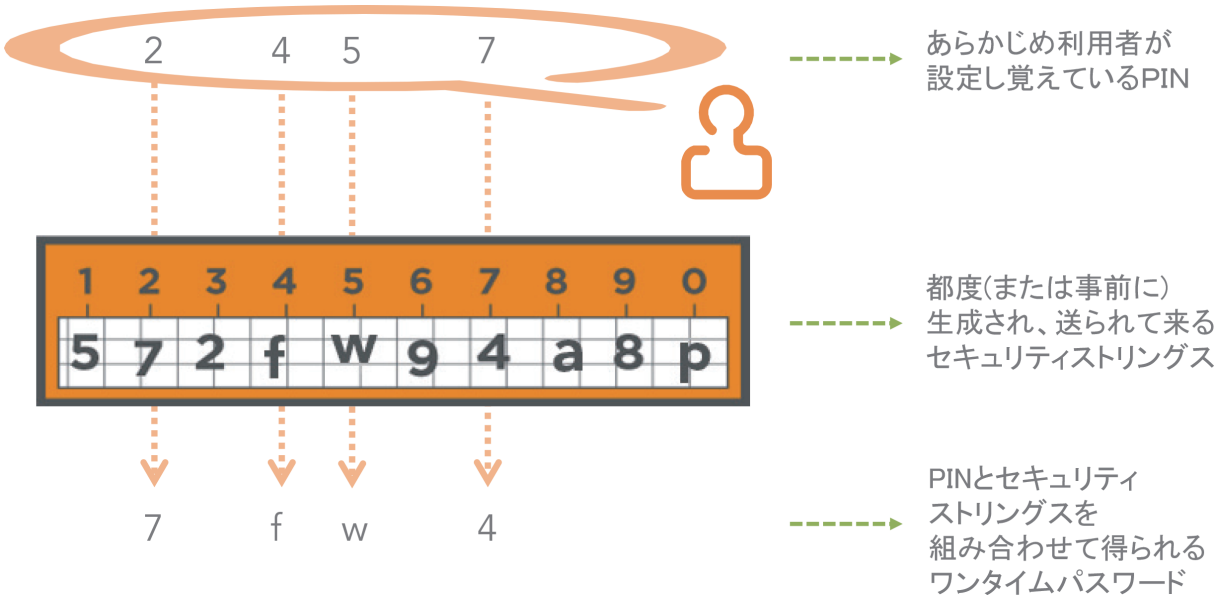


図 1:「PINsafe」ワンタイムパスワード抽出プロトコル

セキュリティストリングスは SMS メッセージや Java アプレット経由、あるいは難読化されたイメージ (TURing イメージ) など、様々な方法でユーザーに送り届けられます。 [*1]

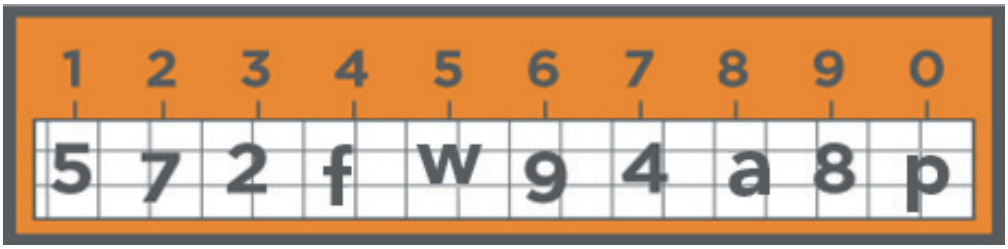


図 2: 難読化したセキュリティストリングス

このアプローチには以下の様な様々なメリットがあります。

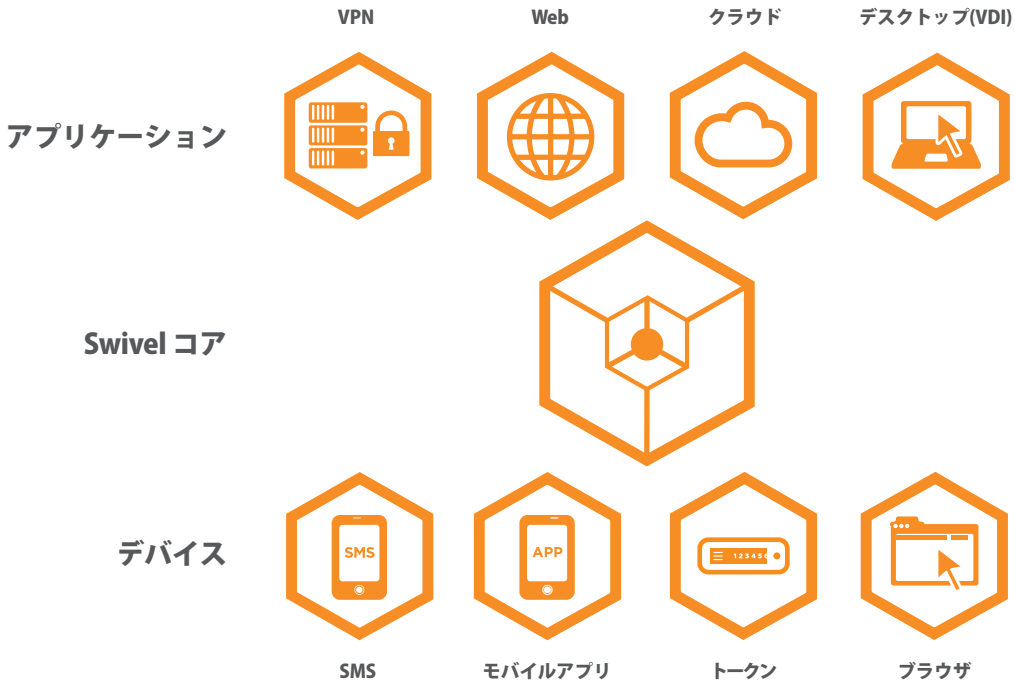
- ユーザーが入力するワンタイムパスワードは毎回異なるため、キーロガーを使った攻撃や多くの中間者攻撃 (man-in-the-middle)、フィッシング攻撃からの防御に有効です。
- ユーザーが PIN そのものを入力することは絶対に無く、その点からも上記の攻撃に対しての防御に効果があります。
- 認証要求を送るチャネルと別のチャネルを使ってセキュリティストリングスを送ることができる (マルチチャネル) ため、中間者攻撃に対抗できます。
- セキュリティストリングスの配信を特定のデバイス (例えば携帯電話) に関連付けることができます。

PINsafe は Swivel ソリューションが持つ非常にユニークな特徴ですが、これを使わなければならないわけではありません。例えば、ワンタイムパスワードの抽出を使わない認証を行うこともできます。

[*1] 難読化されたイメージは Optical Character Recognition (OCR) に対抗できます

Swivel の仕組み

Swivel 認証システムの中核には Swivel Core サーバーがあり、ユーザーデータの管理、要求に応じたログイン情報の生成と管理、認証ポリシーの適用および認証のためのチャレンジの発行 (セキュリティストリングスまたはワンタイムパスワード) を行います。



まず、ユーザーアプリケーション (またはエージェント) が Swivel サーバーに認証要求を行います。エージェントは SSLVPN サーバーであったり、Web サイトにインストールされたエージェントソフトウェアであったり、デスクトップやクラウドサービスで認証を行う Web アプリケーションであったりします。

要求に対し、Swivel は様々な方法でユーザーにセキュリティストリングスを配信します。

- 認証を要求してきた Web フォーム内にセキュリティストリングスを表示。
- セキュリティストリングスをテキストメッセージでユーザーのモバイルデバイスに送信。
- ユーザーが登録したモバイルアプリケーションにセキュリティストリングスをダウンロード。

認証の要求とセキュリティストリングスの配信は、別々の論理チャネルを経由して行うことができます。

Swivel はユーザーの Swivel アカウントに関連したデータを保持するユーザーデータベースを持っています。Swivel サーバーを Active Directory のようなユーザーデータベースと同期させることにより、企業が必要とする Swivel アカウントを簡単に作り出すことができます。

その他、手動でユーザーアカウントを作成したり、Swivel Admin API を使って作成された外部アプリケーションを使ってアカウントを作成することもできます。

異なるエージェント、Swivel サーバーの構成、エンドユーザーデバイスのサポートなど、基本的な Swivel モデルは幅広い異なる形態の認証モデルをサポートします。以下にいくつかの例を示します。

企業向け VPN アクセス、強力な認証

このモデルは VPN ソリューションとしては標準的なものです。Swivel は Active Directory と同期し、必要に応じてユーザーデータベースを Swivel データベースとして生成します。

この場合のアプリケーションは、VPN サーバーになります。VPN サーバーのログオンページが TURing イメージを組み込むよう修正されます。

1. ユーザーがユーザー名を入力し、認証セッションを開始します。
2. ユーザーはセキュリティストリングスを要求し Swivel サーバーから受けとります。セキュリティストリングスは Web ブラウザ上に TURing イメージとして表示されます。
3. ユーザーがワンタイムパスワードを導き出し、入力します。VPN サーバーが RADIUS プロトコルで Swivel サーバーに認証要求を送出します。Swivel サーバーが RADIUS 経由で可か不可かを返します。

Web ポータルへのアクセス、二要素認証

このモデルは Web サイトや Web アプリケーションを保護するための Swivel の利用としては、より一般的かも知れません。ユーザーがポータルに登録した際にポータルが Swivel アカウントを生成します。

ユーザーがポータルのページにアクセスすると、Swivel フィルターが認証が必要かどうかを判断します。認証が必要であれば、そのユーザーはログオンページにリダイレクトされます。

1. アカウント生成または事前の認証要求へのレスポンスとして、Swivel サーバーは SMS 経由でセキュリティストリングスを送ります。
2. ユーザーアプリケーションのログインページがユーザー名とワンタイムパスワードを要求します。
3. ユーザーがワンタイムパスワードを入力し、アプリケーションは Agent-XML API を使って認証要求を行い、Swivel サーバーが結果を返します。
4. Automatic モードでは、ユーザーに自動的に新しいセキュリティストリングスが送信されます。

セキュリティストリングスの配信

前項の例は、Swivel サーバーが認証に際してセキュリティストリングスと PIN を使うことにより、どのようにして強力な認証を実現しているかを説明したものです。

セキュリティストリングスがどのようにして

- 生成
- 配信
- 表示

されるかについては、様々な方法があります。

本セクションでは、Swivel の柔軟性を示すいくつかの方法と、認証を強化するためのやり方についてご説明します。

オンデマンドまたは事前配信

セキュリティストリングスは、エージェントまたはアプリケーションがユーザーの認証要求をする度に発行して送ることもできますが、事前に送っておいて、ユーザーがそれを求められたときにすぐに使えるようにしておくこともできます。

SMS を使った運用におけるデフォルト設定では、ユーザーが認証を行う度に次回のためのセキュリティストリングスを事前に送っておくため、ユーザーは有効なセキュリティストリングスを常に SMS の受信箱に持っていることになります。このモデルでは、Swivel サーバーはユーザーからの認証要求の度に (その認証が受け付けられたか拒否されたかに関わらず)、次回の認証のためのセキュリティストリングスを送っておきます。こうして事前に発行されたセキュリティストリングスは、それが使われるまで、あるいは追加のセキュリティストリングスが要求されるまで有効です。

このほか、ユーザーが認証を要求したときにのみ、セキュリティストリングスを送るという運用もできます。(オンデマンドモード) このモデルでは、ユーザーの代わりにセキュリティストリングスを要求するエージェントが Swivel サーバーのセキュリティストリングスモジュールに要求を出します。

オンデマンドモードでセキュリティストリングスが要求された場合には、有効期間が設定されます。一定時間が経過すると、そのセキュリティストリングスを使って認証を受けることはできなくなります。

オンデマンド方式のメリットは、エージェントによるセキュリティ制御がきめ細かく行えることです。アクセスしているサイトが本物であるときにのみセキュリティストリングスが発行されますから、偽のサイトを使ったフィッシング攻撃からの防御にも有効です。このモデルをさらに拡張して、ユーザーが有効なパスワードを入力しなければセキュリティストリングスが送られないように設定することも可能です。

Swivel ではアプリケーションがセキュリティストリングスにコンテキスト情報を付け加えることが可能なため、セキュリティをさらに強化できます。認証セッションはエージェントの管理下にあるため、エージェントはユーザーが何のために認証を必要用としているかを把握できます。例えば、あるユーザーが発注処理を行うために認証を行おうとしている場合、その情報をセキュリティストリングスの中に組み込むことができます。「$340 の発注のためのセキュリティストリングス」といった具合です。

複数か単独か

セキュリティストリングスの事前送信の場合、一つずつ送るか、複数を一括で送るかを選ぶことができます。例えば、Swivel Module Client は 99 個までのセキュリティストリングスをダウンロードできます。SMS では、最大 10 個までのセキュリティストリングスを二つのメッセージに入れて送ることができます。これにより、認証時にネットワーク接続が無くても認証を行うことができます。

デュアルチャネルかシングルチャネルか

セキュリティストリングスをユーザーのログインダイアログの一部として (例えば VPN のログインページに表示するなど) 表示したり、携帯電話やその他のデバイスに送ることができます。最初のケースでは、セキュリティストリングスは認証と同じチャネルを使って送られるため、シングルチャネルと呼ばれます。二番目のケースでは、セキュリティストリングスは認証要求とは異なるチャネルを使って送られることになり、これはデュアルチャネルということになります。PIN を知るためには、セキュリティストリングスとワンタイムパスワードの両方を知る必要があるため、これら二つを別々のチャネルで送ることにより、傍受が難しくなります。

シングルチャネルモデルでは、セキュリティストリングスは認証を要求してきたエージェントに対して送られます。つまり、セキュリティストリングスを要求してきたエージェントに対して TURing イメージが送られ、そこで認証処理を行うということです。

デュアルチャネルモードでは、セキュリティストリングスは別の論理チャネルを経由してユーザーに直接送られます。これはコアプラットフォームがセキュリティストリングスをトランスポートモジュール経由で特定のデバイスに送ることで実現されるか、ユーザーがモバイルネットワーク経由で特定のデバイスにセキュリティストリングスをダウンロードすることで実現されます。

単一要素か二要素か

単一要素認証は、特定のユーザーがそのユーザーしか知らない情報を知っていることに依存しています。最も一般的な例がパスワードです。二要素認証では、これにその他の要素を追加します。普通はそのユーザーが持っている物、例えばトークンなどです。

Swivel は単一要素にも二要素にも対応できる認証システムです。単一要素の運用ではセキュリティストリングスはユーザーや様々なデバイス上のエージェントで読み出されるため、トークンは必要ありません。

二つの要素を使った運用では、セキュリティストリングスは登録した携帯電話など、特定のデバイスにのみ送られます。例えば、SMS モードではセキュリティストリングスはユー

ザーのアカウントに関連づけられた携帯電話に対してのみの SMS メッセージとして送ることができます。認証のために特定の携帯電話 (第二の要素) を所持していることが必要で、さらにワンタイムパスワードを抽出するための PIN(第一の要素) を知っている必要があります。

攻撃者が二要素認証を破るためには両方の要素を入手する必要があるため、セキュリティ強度は単一要素認証より強力であるとされています。Swivel と PINsafe を使った二要素認証の実装では、PIN は認証プロセスの中で一度も入力されないため、キーロガーなどによる抽出は無意味です。

セキュリティストリングスの生成

セキュリティストリングスは安全性と使いやすさをバランスさせるために、以下の様な様々な方法で生成されます。

- OCR 攻撃に対抗するために、難読化された TURing イメージを生成。
- Swivel モバイルクライアント向けにプレーンテキストで生成。
- 音声に変換して電話で送信。
- セキュリティストリングスを生成するアプリケーションにデータを提供。

ポリシー

ユーザーグループ

Swivel は、ユーザーを異なるグループに分離し、グループ毎に異なる認証モデルを関連づけることのできる機能を持っており、非常に柔軟な運用が可能です。

異なるユーザーグループには Swivel サーバー内で異なる権利を付与できます。これにはどの認証モードを利用できるか (単一、SMS およびモバイルクライアント)、どのアプリケーションで認証を利用できるか、などがあります。

ユーザーはどのアプリケーション、認証モデルを利用できるかについて、一つまたは複数のグループのメンバーとなります。Swivel と Active Directory を使っている場合、ユーザーグループを Active Directory の既存のグループに合わせることができ、これによって Active Directory から Swivel のユーザー権限の管理を直接行うことができます。

結論

Swivel サーバーは柔軟で強力な認証システムとして設計されています。特定の認証トークンに頼らず、トークンの管理やコストに悩まされることが無いため、導入や管理のための時間を劇的に削減できます。

製品は非常に柔軟なため、同じ Swivel システム内で異なる認証ソリューションを異なるユーザーに提供でき、現在および将来の企業の認証システムへのニーズに末永く応えることができます。

また、オープンな設計のため、他システムとの統合が容易で、企業内の様々な IT リソースと統合できます。

これらの特徴により、Swivelは導入リスクの低い認証ソリューションとなっているのです。

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