

シングルチャネルモード

概要

シングルチャネルモードは Swivel 認証システムの最も一般的な導入方法の一つです。このモードでは、ユーザーがチャレンジ(セキュリティストリングス)を受け取るのと同じチャネル(通信経路)を使ってレスポンス(ワンタイムパスワード)を送ります。

本ホワイトペーパーは、このアプローチの柔軟性について概観した上で、管理コンソールから、あるいは html 認証ダイアログのカスタマイズによって実現可能ないくつかのオプションについてご説明します。

 **SecurityStrings**

 **SWIVEL**
the power of knowing

はじめに

シングルチャンネルモードは Swivel 認証システムの最も一般的な導入方法の一つです。このモードでは、ユーザーがチャレンジ (セキュリティストリングス) を受け取るのと同じチャンネル (通信経路) を使ってレスポンス (ワンタイムパスワード) を送ります。

このモードは、通常はブラウザ上の認証ダイアログに TURing イメージを表示する方法で利用されます。

このアプローチには、以下の様な多くのメリットがあります。

- 配備 (導入) が簡単
- 利用が簡単 (使いやすい)
- 表示方法や入力方法を非常に柔軟にカスタマイズできる

本ホワイトペーパーは、このアプローチの柔軟性について概観した上で、管理コンソールからあるいは html 認証ダイアログのカスタマイズによって実現可能ないくつかのオプションについてご説明します。全ての認証フォームにおいて必須とされるのは、Swivel のチャレンジを表示してユーザーからの入力を受け付けることだけです。そのため、このアプローチは非常に柔軟で、多様な導入形態に対応できます。

TURing Image

最も一般的な実装方法は、ログイン画面にセキュリティストリングスのイメージを表示するものです。これは、認証のために Swivel サーバーに接続するログインフォームに html を埋め込むことで実現できます。

このオプションのデフォルトは TURing イメージです。



図 1: TURing イメージ

このとき、異なる背景色や枠線を選んでイメージに「テーマ」を適用する事ができます。(例えば、背景色をモノクロにするなど)

異なるフォントやバックグラウンドを使うことにより、TURing イメージは OCR 攻撃に対して防御力を高めることができます。

この他、イメージの防御力を高めるためには以下の様な方法があります。

- 同じストリングスに対して異なるフォントを使う
- 文字をジグザグに配置して横一列に並ばないようにする
- 文字の太さを変える (アルファモード)

BUTton

TURing のオプションとして、セキュリティストリングスのイメージを 2 次元のパターンで表示する様々な方法があります。図 2 が BUTton レイアウトの例です。2 次元の配列にはユーザーが PIN を覚えやすくする効果があります。例えば、1379 という PIN を設定したユーザーであれば、「Z」のパターンとして覚えることもできます。

異なるバックグラウンド、フォントを使ったオプションもあります。

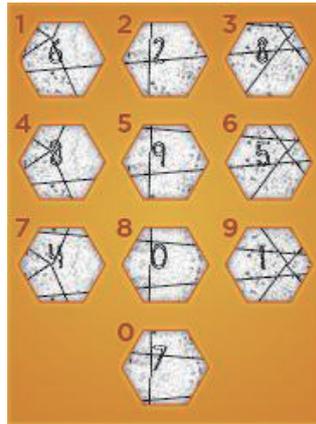


図 2: BUTton 配列のセキュリティストリングスの例

アニメーション

その他のオプションとしては、イメージのアニメーションがあります。TURing イメージのアニメーションを行う主な理由は、スクリーンキャプチャタイプの攻撃に対抗するためです。セキュリティストリングスのキャラクターを点滅させるようにして、どの一瞬にも一部の文字しか表示されないようにすれば、スクリーンショットをとっても一部の文字列しか取得できません。サンプルレートの低いビデオにも同様の効果が期待できます。

アニメーションの設定は Swivel 管理コンソールから行うことができ、以下のようなオプションを設定できます。

- アニメーションパターン
- 一度に表示する文字数
- アニメーションのループ回数



図 3: ジグザグ配置でアニメーションする TURing イメージ

カスタマイゼーション

本ホワイトペーパーでは、基本的には「そのまま使える」オプションを紹介していますが、これらのイメージをどう表示するかをお客様が細かく設定することもできます。

フォントおよびバックグラウンド

全てのイメージで使用されるフォントおよびイメージは Swivel サーバー上のセットリストからランダムに選ばれます。さらに、サーバーが用意したフォントおよびバックグラウンドに制限されずに、自分でそれらをアップロードして使うこともできます。

マスク

その他、カスタマイズが可能な要素としてはマスクがあります。これはイメージ全体の形を決めるものです。TURing イメージについては、マスクは基本的にはフレーム（長方形）で、フレームに様々な色を割り当てることができます。

その他のタイプのイメージについては、マスクは全体の形だけでなく、「ボタン」の大きさや配置を決めることができ、イメージをどのようにユーザーに見せるかを、ほぼ無限に設定できます。

PINpad

PINpad のオプション設定は上記とは違ったアプローチです。セキュリティストリングスが単一のイメージでなく、10 個の独立したイメージとして表示されるからです。これらのイメージが認証フォームと統合され、ランダムに配置された文字盤として表示されます。

何故この様なアプローチがとられるかということ、PINpad はユーザーが覚えている PIN の配置に従ってボタンをクリックすることによって、正しいワンタイムパスワードを入力できるようにになっているからです。

これによりキーロガーによる攻撃に対抗すると同時に新しいユーザー体験を提供します。



図 4: PINpad

タスクバークライアント

ブラウザ上にイメージを表示させないオプションが Swivel タスクバークライアントです。これはシンプルなソフトウェアで、ブラウザ内からセキュリティストリングスを要求してイメージを取得するのと同じ機能を持っています。

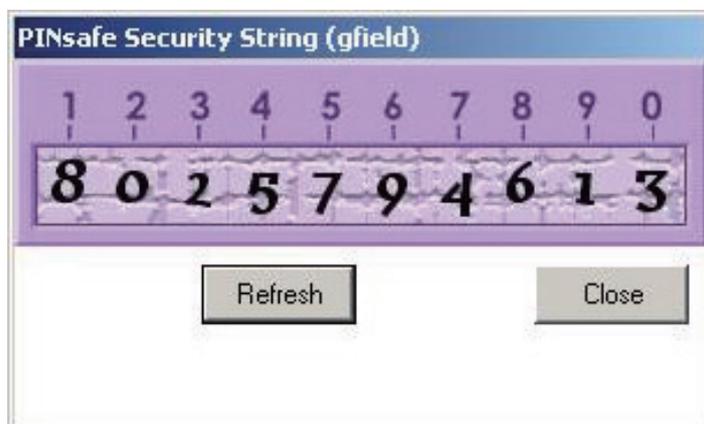


図 5: タスクバークライアントの例

この方法の欠点は、全てのユーザーにクライアントを配布しなければならないことです。しかし同時に、ブラウザ上にセキュリティストリングスのイメージを表示する必要がなくなりますから、man-in-the-browser に対しての防御が可能です。

フォームのカスタマイゼーション

セキュリティストリングスの取り扱いとログインページでの表示方法を変えることにより、ユーザー体験をさらにカスタマイズすることができます。

PINpad 以外のイメージについては、適切な html ファイルを組み込むことによってイメージを表示させることができます。

```
<img src= http://<swivel_ip:port>/proxy/SImage?username=<username>
```

これは、ユーザー名を読み込んで動的に html ファイルを作り出すような JavaScript を作って組み込むことによっても実現できます。以下の様に、ログインフォームに JavaScript の機能 (例えば showTURING など) を呼び出すボタンを付けて呼び出すことなどです。

```
<input type='button' onclick='showTuring()' value=' Get Image' /></td>
```

上記以外のやりかたでも同様のことができます。例えば、ユーザー名フィールドに onblur プロパティを使えば、フォーカスが外れている間、特定のイメージを表示させることができます。

```
<input type="text" id="username" onblur='showTuring()>
```

PINpad

PINpad は 10 個の独立したイメージによって構成されており、ログインフォームによってどのような配列を作り出すことも可能です。例えば、以下の様に単純な表を作って表示するなどです。

```
<table>
<tr>
<td>Username</td><td><Input type="text" id = "username" onblur=showString();></
Input></td></tr>
<tr>
<td colspan =2>
<table>
<tr>
<td onclick=addOtc("1")>
<img id="1"></img>
</td>
<td onclick=addOtc("2")>
<img id="2"></img>
</td>
<td onclick=addOtc("3")>
<img id="3"></img>
</td>
```

showString 機能が適切に配置を行います。

ワンタイムパスワードの入力

ユーザーがどのようにワンタイムパスワードを入力するかについても、細かく設定することができます。TURing や PATtern などについては、デフォルトではキーボードからの入力を想定していますが、PINpad では、ユーザーが PIN をクリックによって入力します。しかし、入力方法はそれらに限定されているわけではありません。

PINpad で設定できるひとつのバリエーションは、PIN をクリックする代わりに、特定の数値のイメージ上にカーソルを一定時間置くことによって入力させることです。これは、ユーザーがキーボード入力やマウスのクリックを必要としないため、キーロガーやスクリーンキャプチャなどの攻撃に対しても防御できることが特徴です。ほとんどの Swivel の実装形態において、標準の html/JavaScript を用いて実装することができます。

この PINpad の入力方法と TURing イメージによるセキュリティストリングスの表示を組み合わせることが可能です。セキュリティストリングスを TURing イメージで表示し、PINpad のボタンにカーソルを合わせることで、キー入力やマウスクリック無しにワンタイムパスワードを入力することが可能になります。

結論

シングルチャネルオプションの考え方は非常にシンプルです。ユーザーにセキュリティストリングスを含んだイメージを表示し、ユーザーがそれに対して適切な対応をすることで認証を行います。非常に単純なモデルですが、様々なイメージ表示の方法や入力方法を組み合わせることにより、お客様のご要望に合うよう簡単にカスタマイズできます。