Pinpad

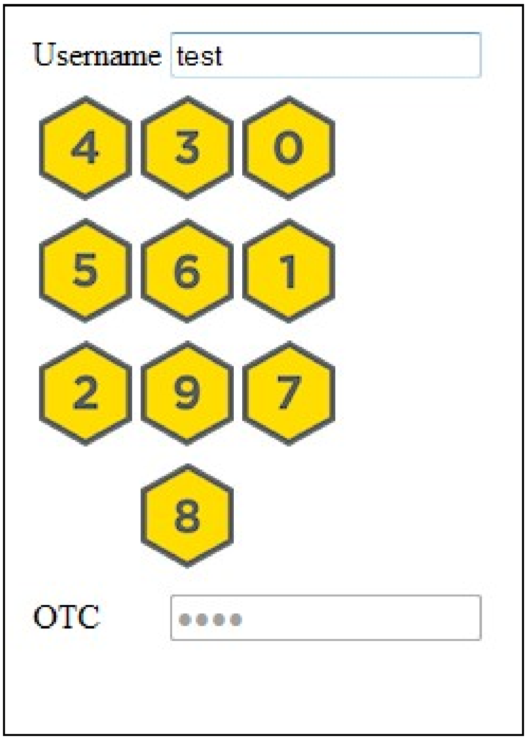
Contents

History

29th May 2012: Updated to include the fact that when you click your PIN the form is populated with button position not button contents.

Introduction

PINpad is an alternative way of implementing browser/image based authentication. It is different from other forms such as TURing, in that the user has to click a scrambled keypad in order to authenticate. In this model, the user has to click on the images that represent their PIN, rather than perform a one-time code extraction. Because the user has to click their PIN, their PIN is not vulnerable to key-logging and because the entry pad is scrambled differently every time, attacks that log where mouse clicks are made are not a threat as the clicks required are different for every authentication.



Username test

OTC ••••

Key to this solution is the fact that when the user clicks the digit that represents their PIN, the form is not populated with the digits that represent that PIN, but with the positional references of the buttons. So in the example a user clicking their PIN of 2-4-6-8 would cause the form to be populated with 7-1-5-0. Thus the PIN cannot be directly intercepted.

Prerequisites

Swivel 3.9.2 or later. Earlier versions require the Swivel PINpad proxy software, see Integrating PINpad for versions prior to 3.9.2.

Numeric security strings only

Implementation

Versions prior to 3.9.2 require the use of the Proxy server. Versions 3.9.2 onwards have the PINpad built into the Swivel application.

The PINpad is usually presented to the user through images on port 8443 (or 443 using a Port Address Translation) from the Swivel appliance.

Swivel Server Configuration

On the Swivel instance under Server/Single Channel, set Allow session request by username to Yes.

Using PINpad

The format of the request is via an http get.

eg <img src = https://<serverIP>:<port>/proxy/SCPinPad?username=test&padno=8370:3>

Where 8370 is the unique session key and the 3 indicates it is the 3rd button image that is being requested.

This approach has been adopted as it mirrors the methods used for retrieving single-channel images via the proxy, albeit that this method requires 10 different images rather than a single one.

As 10 different images are requested the html that renders login page can place and arrange these images as required.

Here is some example html. Note that the showString function only loads digit pinpad0, and the rest are loaded in the onload event for that image. This ensures that only 1 session is created, as described in the Known Issues section.

```
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=ISO-8859-1">
<title>Insert title here</title>

<script type="text/javascript">

function showString() {
        var session,name,img;
        name = document.getElementById("username").value;
        session = Math.ceil(10000*Math.random());
        img = document.getElementById("pinpad0");
        img.onload = function() { showString2(session); };
        img.src = "http://localhost:8080/proxy/SCPinPad?username=" + name + "&padno=" + session + ":0";
}

function showString2(session) {
        var name,n,img;
        name = document.getElementById("username").value;
        for (n = 1; n<10; n++){
                img = document.getElementById("pinpad" + n);
                img.src = "http://localhost:8080/proxy/SCPinPad?username=" + name + "&padno=" + session + ":" + n;
       }
}
function addOtc(digit){
        var otc = document.getElementById("otc");
        otc.value = otc.value + digit;
}

function clearOtc() {
        var otc = document.getElementById("otc");
        otc.value = "";
}

</script>
</head>

<body>
<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="pinpad1" src="PinpadBlank.png" />
</td>
<td onclick='addOtc("2")'>
<img id="pinpad2" src="PinpadBlank.png" />
</td>
<td onclick='addOtc("3")'>
<img id="pinpad3" src="PinpadBlank.png" />
</td>

</tr>
<tr>
<td onclick='addOtc("4")'>
<img id="pinpad4" src="PinpadBlank.png" />
</td>
<td onclick='addOtc("5")'>
<img id="pinpad5" src="PinpadBlank.png" />
</td>
<td onclick='addOtc("6")'>
<img id="pinpad6" src="PinpadBlank.png" />
</td>

</tr>
<tr>
<td onclick='addOtc("7")'>
<img id="pinpad7" src="PinpadBlank.png" />
```

```
</td>
<td onclick='addOtc("8")'>
<img id="pinpad8" src="PinpadBlank.png" />
</td>
<td onclick='addOtc("9")'>
<img id="pinpad9" src="PinpadBlank.png" />
</td>

</tr>
<tr>
<td onclick='clearOtc()'>
<img src="PinpadClear.png" />
</td>
<td onclick='addOtc("0")'>
<img id="pinpad0" src="PinpadBlank.png"></img>
</td>
<td onclick="showString()">
<img src="PinpadRefresh.png" />
</td>
</td>

</tr>
</table>


</td>
</tr>
<tr>
<td>OTC</td><td><input type = "text" id="otc"></input></td>
</tr>

</table>
</body>
</html>
```

PINpad Change PIN

When using Pinpad with a Change PIN page, there is an additional complication in that there are 3 OTC fields to fill in. This section does not describe how to implement this in your own code: rather, it describes how it has been implemented in Swivel code.

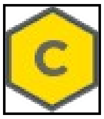
The standard used in those Swivel applications where Change PIN with Pinpad has been implemented is that the old OTC field is selected when the Pinpad image is first displayed, and is highlighted (in green). To select the other OTC fields, the user needs to click on the **label** of the field, NOT the field itself, in order to activate it. The active field (i.e. the one that Pinpad will populate) is always shown in green.

Enhanced Implementations

See also Single Channel Customisation How to Guide#PINpad Editing

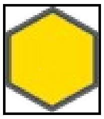
PINpad Clear and Refresh

The example above uses the following images, which you will need to copy to your web server, if you use them. Where these are implemented, they have the following effect:



The **C** button clears the OTC field, i.e. removes any input. For change PIN, it only clears the active OTC field.

The **R** button refreshes the Pinpad image. It displays a new security string, and removes all input from all OTC fields.



You may want to use this image as a placeholder for an empty Pinpad button.

Editing PINpad images

See Single Channel Customisation How to Guide

Integrating PINpad for versions prior to 3.9.2

This page contains the latest Appliance proxy software. You will need to extract it from the zip file before deploying.

The web.xml within the PINsafe context needs to be edited to allow the proxy to retrieve a security string.

The following entry needs to be added in the servlet-mapping section and then restart Tomcat. (Always take a back-up of this file before editing it)

```
 <servlet-mapping>
  <servlet-name>SCText</servlet-name>
  <url-pattern>/SCText</url-pattern>
 </servlet-mapping>
```

This updated proxy retrieves a security string from the Swivel server and serves it, digit-by-digit as requested by the login page.

In order to ensure that each digit is only served once, the request of each digit must include a unique sessionkey.

This sessionkey should be the same for each digit requested for a given pad but then different for each pad requested.

Testing

Using a valid username should allow a valid PINpad to be generated.

Known Issues

Multiple Sessions

There is an inherent problem with displaying PINpad on a web page, in that a user session is started automatically by the first digit to be displayed. Since all digits are generated in quick succession, there is the possibility that more than one session is generated. This is particularly a problem in HA solutions where appliances are load balanced, due to slow session replication.

The preferred option is to generate a session explicitly using AgentXML, and then to use the session ID to generate the images. This guarantees that there is only one session. However, this solution requires that the web front end for the integration concerned is capable of server-side code, as the session start request has to come from the front end, not directly from the appliance. If this is not possible (as is the case with several common VPN gateways), an alternative is to display a single digit first, and display the rest in a separate JavaScript function called from the onload event of that image. The example above shows one way of accomplishing this.

In Swivel 3.9.2 a bug prevents non Swivel users authenticating where integrations allow non Swivel users to authenticate without Swivel credentials. If this option is used, then the proxy should be used, or upgrade to 3.9.3 or later.

The PINpad is case sensitive and this can cause problems with the PINpad when used directly against Swivel when a username PINpad is requested. Using Session or the Swivel proxy overcomes this issue.

Troubleshooting

PINpad is slow?

- Are you using a signed certificate on the Swivel server and does the URL hostname match the site name of the cert?
- Has an internal Certificate Authority has been moved or removed and it is reaching a time out value looking for the CA.
- If the Swivel PINpad is proxied through a Windows server install/import the Swivel wildcard cert into the certificate manager panel of the Windows Server (where the ASP file is proxying the Swivel image) so that it recognises the certificate. Delays of this nature may be caused by initial certificate validation attempts.
- Check DNS settings
- Is there any Load balancing, such as DNS round robin

Multiple Digits Appearing on the PINpad

Resolved in version 3.10.2 - It is recommended to upgrade to 3.10.2 or later. This was caused by upper and lower case issues.

Red Cross Appears instead of PINpad image

Right click on the image to verify the URL for the image, the URL should appear similar to the below depending on IP address and port:

```
http://127.0.0.1:8080/pinsafe/Pinpad?username=testuser&padno=32:3
```

The URL can be entered into a web browser and for a valid username should generate an image, and a corresponding entry in the Swivel log viewer.

Only some of the PINpad digits appear

PINpad only works with numeric security strings, other characters are not displayed, set the security strings to be numeric on the Swivel administration console.

Session start failed for user: <username>, error: Single channel session request by username is disabled.

On the Swivel instance under Server/Single Channel, set Allow session request by username to Yes.

Only digits one to six are displayed

If only digits 1-6 are displayed then the user is probably a PINless user and should not be allowed to use single channel access, or should be made a PIN user.