Voice Innovate Corporation

SecurLogin Overview

18 July 20118 Rev 1.0

1.0 Intended Audience

It is assumed that users of this document are technically oriented by nature and are familiar with telephony and web based infrastructures and their associated components.

2.0 Overview

Smart cards by nature can be used by individuals other than the registered user by choice of the registered user or by fraudulent means. For example, a user can give their token and PIN to a friend.

The SecurLogin Application is intended to add a third factor of authentication to existing Smart Card login processes using Voice Biometrics.

Much like finger prints are unique to an individual, so is their voice.
By using voice biometrics, only the registered user can authentic with the smart card.
Voice authentication also means “User accountability”.

Login processes secured by SecurLogin leverage Smart card technology and add voice biometric authentication to the Login process.

Users typically access a secured web page, provide their smart card credentials and then are prompted to call the SecurLogin IVR to perform voice authentication.

Once voice authenticated, the user is then given access to the secured resource.

3.0 SecurLogin Walk Through

This is a short description on how to use SecurLogin with a existing web site where we have altered the authentication mechanism to use smart card and voice authentication factors via the SecurLogin application.

This document assumes that the SecruLogin servers have been installed, the user account has been configured by the system administrator and the user is ready to verify.

- **Setting Up the Web Client You Want to Protect**

The setup to replace the existing authentication on a client web application is relatively easy because we use OpenID which is an industry standard for authenticating clients on a remote system. An OpenID application programming interface (API) is available for all programming languages as well client plugins are available from most web applications. In this example we used the libraries available from http://openid.net/developers/libraries/ to protect the example site "Example Corp. Secure Files".

An important additional step is that we don't want to allow just any OpenID server to authenticate for our web application so we set the configuration of our web application to only use our SecurLogin URL (Uniform Resource Locator).

- **Accessing the Web Application**

The user access the web application and enters the SecurLogin username into a form field and then presses the submit button. The client web application and SecurLogin application create a shared secret using cryptography keys[1] which is used to sign and verify all following messages between them.

[1] Diffie-Hellman key exchange

Authentication Redirect

The user gets redirected to the SecurLogin web site and it checks to see if the user has been logged in[2].

Our user has not been so, they continue with the next step.

[2] A user is authenticated across all your web applications when they authenticate with SecurLogin

- **Smart Card Authentication**

The user inputs the one time login from the smart card and presses the "Login"

button. Then the token is authenticated and if it's valid the user continues to the next step. If it's not valid the user needs to continue trying according to the policy of the token domain.

- **Voice Authentication**

The user now calls the phone number displayed on the page. When they call in they are asked to put in the smart card serial number and then they are prompted to repeat up to 6 random digits.

If your account has been configured with a callback number you'll also see a button which when clicked will have the system call you. The page after that is in the style of the other ones and reads "You are being called at (555) 555-5555 for voice authentication"

After successful authentication against the previous enrolled and stored voice print they continue to the next step.

- **Authenticated Redirect**

The SecurLogin application directs the user back to the page they are authenticating from and the client application verifies the information using our cryptographic keys. The user is granted access and authorization continues as normal.

5.0 Topology

SecurLogin leverages existing Corporate Web Servers and Smart Card Servers. Optionally it can leverage an existing Corporate Database using ODBC connectivity.

The following diagram illustrates a sample implementation of SecurLogin within a corporate infrastructure.

Typically the Web and Smart card servers are part of the corporate infrastructure while SecurLogin application provides the SecurLogin IVR and the mechanisms required to customize the corporate Web server and if a corporate database is to be leveraged the information required to customize the database for use by SecurLogin.

A minimum of one SecurLogin IVR must be implemented, but multiple SecurLogin IVR's can be implemented to provide scalability for call volume, load balancing, and fault tolerance.