Remote Veterans Apnea Management Portal

TECHNICAL OVERVIEW

SECURITY GUIDE

Department of Veterans Affairs,
REVAMP
VA118-12-Q-0582

INTELLICA CORPORATION
209 W. POPLAR
SAN ANTONIO, TEXAS 78212

04/18/2013

This Page Intentionally Left Blank

Intellica Corporation ◆ 209 West Poplar Street ◆ San Antonio, Texas 78212 ◆ Phone (210) 341-3101 ◆ FAX (210) 271-7860

Table of Contents

Intellica Corporation ◆ 209 West Poplar Street ◆ San Antonio, Texas 78212 ◆ Phone (210) 341-3101 ◆ FAX (210) 271-7860

Intellica Corporation ◆ 209 West Poplar Street ◆ San Antonio, Texas 78212 ◆ Phone (210) 341-3101 ◆ FAX (210) 271-7860

Table of Figures

Intellica Corporation ◆ 209 West Poplar Street ◆ San Antonio, Texas 78212 ◆ Phone (210) 341-3101 ◆ FAX (210) 271-7860

Change Log

Date	Version #	Author	Revision Description
04/18/2013	1	Intellica	Created

Intellica Corporation ◆ 209 West Poplar Street ◆ San Antonio, Texas 78212 ◆ Phone (210) 341-3101 ◆ FAX (210) 271-7860

Introduction

This document is the Security Guide for the VA REVAMP application. It describes security related items and identifies possible threats and counter measures.

Decompose the Application

REVAMP System Architecture

1. An Internet Explorer 9.0 Web Browser HTML5 compatible and capable of navigating and displaying ASP.NET pages and running client side JavaScript.

2. A Microsoft Windows 2008 Server running Internet Information Server 7 (IIS) and ASP.NET 4. This is the application server that hosts the Web application.

3. A Microsoft Windows 2008 Server running Oracle. This is the database server for the application.

4. TIU and MDWS are used for authentication and access to VistA data.

Intellica Corporation ◆ 209 West Poplar Street ◆ San Antonio, Texas 78212 ◆ Phone (210) 341-3101 ◆ FAX (210) 271-7860

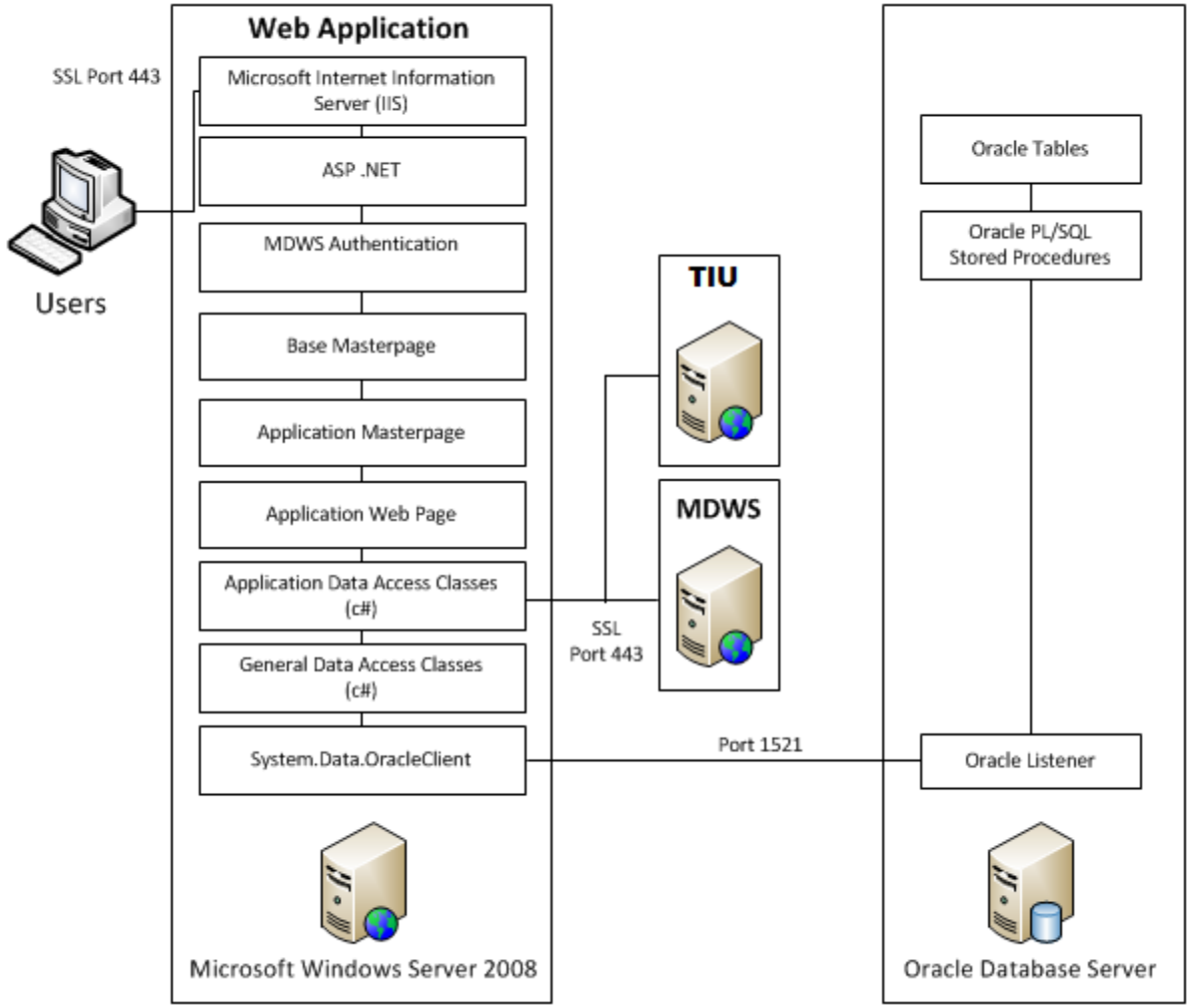

Figure 1 – REVAMP Overview

User Registration

The REVAMP tool uses MDWS to authenticate users. The user must have a MDWS account to access the application. No user registration capability exists in the application.

User Login

The user must present valid MDWS credentials to login. When the user logs in to the system, a database session record will be created. Requests after logging in require a match in the session table on IP address, DBSessionID and client IP address. If the MDWS connection times out for any reason, the user will be prompted to login again.

User Roles

The REVAMP tool will use MDWS roles to determine permissions for the application. Roles are yet to be determined.

Access to pages

Page access will be restricted by user role. Whenever a user attempts to access a page, the database is queried to determine if the user's role meets the requirement for accessing the page. If the user is unable to access the page, the user is logged off.

Auditing

Every stored procedure call made by the application is audited. The following items are stored in the database on every audit: database session ID that made the call, client IP from where the call originated, user ID that made the call, date and time the call was made, stored procedure called and parameters passed to the stored procedure. The parameters passed to the stored procedure are will be encrypted before storage.

Intellica Corporation ◆ 209 West Poplar Street ◆ San Antonio, Texas 78212 ◆ Phone (210) 341-3101 ◆ FAX (210) 271-7860

Encrypting Data at Rest

User Name/Password Encryption

User names and passwords for the application are stored encrypted at rest as follows:

The procedures PCK_FX_SEC.InsertFXUser and PCK_FX_SEC.UpdateFXUser take two input parameters: pi_vUserName and pi_vPassword. These parameters are 3DES encrypted from the application before they are passed. The key used for the 3DES encryption is stored encrypted in the connectionStrings section of the web.config file as follows:

```
<add name="SEC" connectionString="keygoeshere"/>
```

The table fx_user stores the user name and password encrypted at rest in the user_name and password fields.

Patient Data Encryption

All stored procedures that need to encrypt or decrypt patient data are passed the encryption key in the pi_vKey parameter. The data is AES 256 encrypted from the database using the fnc_utl_encstr function and decrypted using the fnc_utl_decstr function. The key used for the AES 256 encryption is stored encrypted in the connectionStrings section of the web.config file as follows:

```
<add name="Key" connectionString="keygoeshere"/>
```

The procedures PCK_PATIENT.InsertPatientDemographics and PCK_PATIENT.UpdatePatientDemographics take all demographic information as un-encrypted parameters and encrypt this data before storing in the patient_demographics table. The following fields are encrypted at rest:

- FIRST_NAME
- MI
- LAST_NAME
- FMP
- SPONSOR_SSN
- SSN
- DOB

Intellica Corporation ◆ 209 West Poplar Street ◆ San Antonio, Texas 78212 ◆ Phone (210) 341-3101 ◆ FAX (210) 271-7860

- EMAIL

Stored procedures that return encrypted patient data must first decrypt the data using the key passed in and the fnc_utl_decstr function.

Example: fnc_utl_decstr(t.LAST_NAME, pi_vKey, t.PATIENT_ID)

Running Oracle Jobs that Require Encryption Key

All stored procedures that must run as jobs are defined in the PCK_JOBS package.

Stored procedures that run as Oracle jobs cannot be passed the key directly; in this case we must go get the key before calling the procedure. The function below will retrieve the encrypted key from a file in the database server system directory and unencrypt it for use.

```
sys.ic_utl_gk('DRDB', v_vKey);
```

A wrapper procedure is created for each job. This wrapper goes and gets the key and passes it to the stored procedure that needs to run from the job.

Example:

```
procedure ImportRESMEDData
is
        --get the key
        sys.ic_utl_gk('DRDB', v_vKey);

        --run the sp
        PCK_CPAP_IMPORT.ImportRESMEDData(
                v_vKey,
                nStatusCode,
                vStatusComment);
end;
```


Intellica Corporation ◆ 209 West Poplar Street ◆ San Antonio, Texas 78212 ◆ Phone (210) 341-3101 ◆ FAX (210) 271-7860

Remote Systems

The VA REVAMP Tool uses the following remote systems:

1. MDWS

Mail Groups and Alerts

Outgoing only

Text Message server

Outgoing only

Patient-facing application

Same architecture as REVAMP

Threats and Countermeasures

Spoofing Identity

"Identity spoofing" is a risk for applications that have many users but provide a single execution context at the application and database level. In particular, users should not be able to become any other user or assume the attributes of another user. The following measures are in place to prevent spoofing Identity:

1. The REVAMP will use a "limited privilege" database account

2. Connection to the database occurs in only one location in the BaseMaster page

3. All Master pages derive from the BaseMaster page. BaseMaster consolidates security checks and the one and only connection to the database for each page load.

Intellica Corporation ◆ 209 West Poplar Street ◆ San Antonio, Texas 78212 ◆ Phone (210) 341-3101 ◆ FAX (210) 271-7860

4. All Pages use "MastePage" which derives from BaseMaster.

5. The user must present valid MDWS credentials to login

6. When the user logs in to the system, a database session record will be created. Requests after logging in require a match in the session table on IP address, DBSessionID and client IP address.
7. Page names and roles that can access the page will be stored in the fx_page_access table. If the user is not authorized to view a page they are logged off the system.

8. User information such as role, id etc. are retrieved from the database on every page load, they are not cached in session or view state. To retrieve user information the user must be logged in and pass in a valid ASP .Net session id, DBSessionID and client IP address. If at any time a match is not found, the user is logged off the system.

9. BaseMaster also protects against CSRF attacks. When the user logs in, a challenge token will be created on the server. If the user sends a GET request to the server, the token sent in the response. If the user sends a POST request to the server, the token from the POST must match the token on the server. If the tokens do not match the user is logged off. No sensitive actions on executed on GET requests.

Repudiation

Users may dispute transactions if there is insufficient auditing or recordkeeping of their activity.

1. All changes to data are logged in the fx_audit table. Security events such as page access, successful/unsuccessful logins will also be stored in the fx_audit table.

Denial of Service

Application designers should be aware that their applications may be subject to a denial of service attack. Therefore, the use of expensive resources such as large files, complex calculations, heavy-duty searches, or long queries should be reserved for authenticated and authorized users, and not available to anonymous users.

Intellica Corporation ◆ 209 West Poplar Street ◆ San Antonio, Texas 78212 ◆ Phone (210) 341-3101 ◆ FAX (210) 271-7860

1. Only the home pages of the application are accessible by anonymous users. The home pages only allow a user to log in.

Elevation of Privilege

If an application provides distinct user and administrative roles, then it is vital to ensure that the user cannot elevate his/her role to a higher privilege one. In particular, simply not displaying privileged role links is insufficient. Instead, all actions should be gated through an authorization matrix, to ensure that only the permitted roles can access privileged functionality.

1. Page access is regulated by the user's role.

2. Higher privileges and roles are disabled based on the user's role.

Session Hijacking

Session tokens can be compromised by various methods. Using predictable session tokens can allow an attacker to hijack a session in progress. Session sniffing can be used to capture a valid session token or session id, and the attacker uses this session information to gain immediate unauthorized access to the server which is a loss of confidentially and potentially a loss of integrity. Also, the Man-in-the-Middle (MITM) attack can be accomplished over a TLS connection with a session in progress.

1. Session IDs are 24 character alphanumeric strings created by ASP.NET using the Random Number Generator cryptographic provider. This makes it difficult for an attacker to guess a valid Session ID.

2. All communication between the client browser and the application server is encrypted using SSL. This prevents session sniffing by an attacker.

3. All requests are checked for a valid Session ID. If a valid Session ID is not presented with a request, the session is abandoned for the matching client IP.

Intellica Corporation ◆ 209 West Poplar Street ◆ San Antonio, Texas 78212 ◆ Phone (210) 341-3101 ◆ FAX (210) 271-7860

Canonical Representation Vulnerabilities

Canonical representation issues arise when the name of a resource is used to control resource access. There are multiple methods of representing resource names on a computer system. An application relying solely on a resource name to control access may incorrectly make an access control decision if the name is specified in an unrecognized format.

1. The application's webpages are the only resources that have their access controlled by their name. The URL will be decoded by HttpUtility.UrlDecode before the comparison is made. If the webpage is not recognized, then access is denied.

Cross Site Scripting Vulnerabilities

Cross site scripting (XSS) vulnerabilities exist when an attacker uses a trusted website to inject malicious scripts into applications with improperly validated input.

1. ASP.NET validates all input for XSS attacks if page validation is on. If ASP.NET detects potentially hazardous input, then an exception is thrown.

SQL Injection

SQL injection is a code injection technique that exploits a security vulnerability occurring in the database layer of an application.

1. The REVAMP will use a "limited privilege" database account.

2. All calls to the database are through Oracle Stored Procedures.

3. All SQL inside of Stored Procedures use bind variables, recordsets are opened using the "open" command and statements are executed using "execute immediate."

Intellica Corporation ◆ 209 West Poplar Street ◆ San Antonio, Texas 78212 ◆ Phone (210) 341-3101 ◆ FAX (210) 271-7860