Password Management Automation

Mukundan Sundaresan

Practical Assignment for GSEC Certification v1.4b Option 2

June 30, 2004.

Abstract

The objective of this paper is to discuss Password Management Automation and how it can be handled in small, medium and large scale organizations. Password Management is one of the key factors in every organization. People work in different positions with different responsibilities and they should have appropriate access to perform their daily work. In order to access different resources in the enterprise, the user will be responsible for providing necessary credentials. Password Management policy is one of the processes of Identity Management. The likelihood of forgetting password is highly possible due to its complexity. Users are encouraged to create strong password and also use different passwords to access different systems. This paper highlights the various advantages like ease of use, cost-benefits, utilization of technological growth in developing a software solution with Security, and meets the business needs. I played the Technical Team Lead role in this project and I was responsible for developing the System Architecture and Design for all the applications described below.

Introduction

Password Management Automation is achieved through the creation of various tools and processes. In an organization, a user is prompted for an id and password before he/she is allowed to access the authorized resources. When an id is provisioned for new employee, the id is set with a default password and the employee will be expected to change the password as per the company's security policy. Password Management helps increased security and productivity. Managing user's password is the one of the important aspects of security. Password Management is the most, that affects a large number of people in the organization and therefore it should be relatively easy to implement and roll-out. It is very expensive to maintain user's password. Several organizations are going towards tools for self-service password reset and Help-Desk password reset. Apart from this there are some organizations which are trying to incorporate the concept of Single Sign-On. Password Synchronization is another process to overcome the hurdles of Password Management. Even though Single Sign-on is a powerful process, it is more vulnerable. If a hacker gains the password for the primary login of a user, then he/she will gain access to all the resources that the user is authorized to. Therefore lots of organizations are scrutinizing the negative impact of Single Sign-On. There could be various systems in different platforms like Windows, UNIX, and Mainframe, where the user has to login explicitly to each system. To handle this, our organization decided to develop tools and automate the process of password management. This would result in cost savings for the enterprise. The user will have access to the tool anytime, which will eliminate support calls for password reset.

Password Management Challenge

Due to the availability of several computing systems, users tend to forget their password easily. On an average 30% of the support calls received by the help-desk are related to password reset. End-users are provided access to different systems and therefore they find it too difficult to manage their passwords, which results in the impact of support cost, productivity, security and privacy.[1]

In an enterprise there are sensitive and non-sensitive information, which are stored in multiple environments. Appropriate access should be granted to employees in the organization to various systems without security breach. Based on the company's security policy, multiple identities and multiple passwords are held to access different systems in the organization. This results in user not remembering all passwords. Report shows that 70 percent of the users have problems with their password on a monthly basis and more than 30 percent of the help-desk calls are password related. This costs around $200 - $300 per user, per year. Critical Path provides solutions which integrate with enterprise applications. They are:

- Password Policy Management – Consistent Password Policy, strengthening the effectiveness of passwords and increasing information security.

- Password Synchronization – Passwords are synchronized and therefore very few passwords to remember.

- Password Self-Service – Users are provided with tools, which can be used on their own.[2]

Password Management Policies

Password Management policies are enforced by the organization based on their security policy. University of Auckland has highlighted the following policies.

- User Id, Personal Identification Number (PINs) and passwords must be strictly controlled.
- Since they are confidential they should be protected accordingly.
- Effective password management system should be incorporated.
- End users must follow good practices when managing their PINs or passwords.[3]

---

[1] See "Password Management Challenge."
[2] See "Password Management."
[3] See "Information Security Management."

SecureLogin Single Sign-On Overview

Protocom SecureLogin Single sign-On provides the flexibility of logging into their applications, websites, and mainframe systems with a single login. Therefore users do not have to remember multiple passwords, which reduce the risk of forgetting password. The user has to login into the network with Windows credentials and SecureLogin retrieves the password, which is stored in an encrypted form in the workstation and sends it to the respective platforms. This increases the user productivity and reduces the help desk calls greatly. It is highly cost-effective and secure.[4]

Password Management Process & Tools

Here are the building blocks of Password Management. To manage the process of Password Management, the following tools have been designed and developed to meet the enterprise needs. The process and tools are divided into four parts:-

A. Password Expiration process
B. Self-Service tool to change the user's password.
C. Help-Desk tool managed by administrators to reset user's password.
D. Self-Service tool for Password Reset.

A. Password Expiration process

Depending on the organization's security policy the password expiration process will be determined. Once the password has expired the user will be re-directed to a page where he/she will be expected to change the password. Only after changing the password, the user will be allowed to access any authorized resources. Based on the organization's security policy the password expiration process could take place once in 60 days or 90 days or 120 days. The Self-Service tool and Help-Desk tools are developed as a thin-client web based application using Active Server Pages (ASP) and Visual Basic. The ASP pages are used to develop the front-end and VB is used to develop mid-tier COM (Component Object Model) components.

B. Self-Service tool to change the user's password

This page helps the user to change the password at any time. The user's identity is validated by the operating system, which is used as the source for authorization. To ease the process of changing the password, a web tool is developed and therefore the user has the ability to change the password at will. Strong Password is one of the important factors that are taken into consideration by several organizations. According to the organization's security policy the rules can be enforced for a password change. Some of the best practices information is shown below, which could be applied to any type of organization.

[4]See "SecureLogin Single Sign-On."

The password must meet the following guidelines to ensure that they are strong.

- Passwords must be eight characters or more.
- Passwords must contain at least one upper or lowercase character.
- Passwords must contain at least one digit, and at least one numeric value.
- Passwords must contain at least one special character. (This should be handled according to the compatibility of various systems in the organization.)

The password must not contain the following.

- Passwords must not be a dictionary word.
- Passwords must not be a user name or login ID.
- Passwords may not contain more than two paired letters (e.g. abbcdde is valid, but abbbcdd is not).[5]

If the above mentioned criteria's are met, then it could be considered as strong password.

User Interface Architecture for Self-Service Tool

The User Interface is developed using ASP, containing VBScript for the server-side, JavaScript for client-side, with HTML, XMLHTTP, and XML for input and output.

The application has the following web pages:

- Start.ASP
- Redirection.asp
- ChangePassword.asp

When the user launches the Internet Explorer, Start.asp is called, which identifies whether the user's password has expired or not and the control is passed to the Redirection.asp, if the user's password has expired, otherwise the user will be re-directed to the appropriate site. The Redirection page retrieves the user information from the directory based on the credentials passed by the browser. The password guidelines are validated by using JavaScript. Additional validations are performed to ensure that the user is not trying to change the new password, same as the old password. The ChangePassword.asp will instantiate the component and passes the user id, old and new passwords to the component. Once the password is successfully changed, a web model dialog box is displayed and the current instance of the browser is closed. The user should authenticate again with the new password.

[5] See "Password Management Best Practices."

Data Binding

ChangePassword.asp page sends and receives the data to and from components in XML format. This page uses XMLHTTP to post the XML data which in turn passed to the component for processing. The data is received as XML string which is parsed using XML parser and the information is displayed on the page. The application uses Microsoft XML DOM object to transmit data between the front-end and back-end.

Pop-up Windows/Browser

The success or failure (errors) messages are displayed in a Modal Web Dialog box. If a critical error occurs, then the error message is displayed on the browser, which provides appropriate contact information to resolve the issue occurred.

Images

The following two images are used on the page.

The size of the controls and tables on each screen are in percentages so the windows can be resized and contents are still visible.

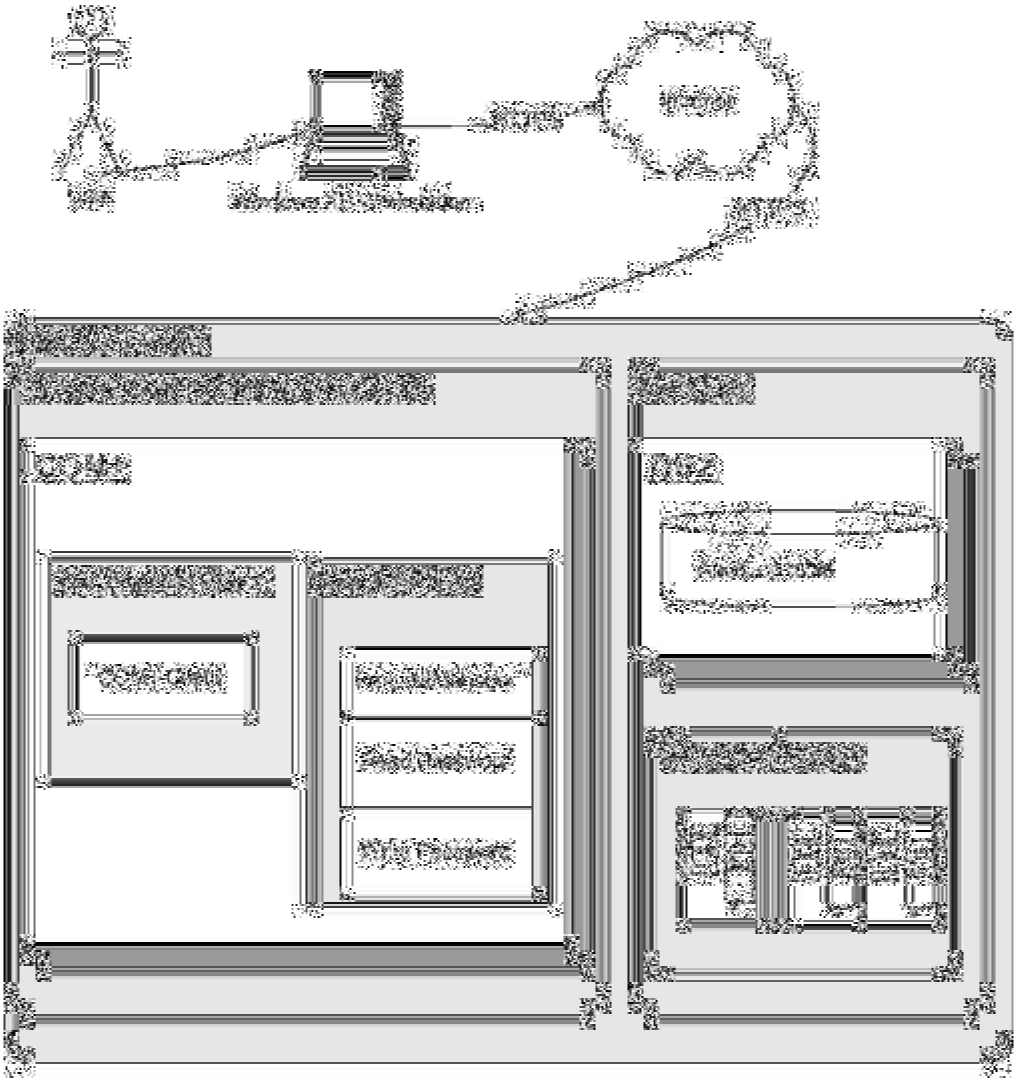
Error Processing

There are two types of errors: Error returned by component and error occurred on ASP page. When an error occurs on a call to the component, the ASP page will handle the error. An appropriate error message will be sent back to user, which includes logging and packaging the error data in an xml format and then pass it to the error page. When an error is returned from the component, the error xml received, is passed to the error page that will be displayed on the user's browser as a model web dialog window, if it is related to authentication failure, whereas if it is a critical error, it will be directly displayed on the browser. Error logging is handled by the system on the mid-tier server.

Help option

A help option is provided for the user to handle user-defined errors, which can be resolved by using this. The help screen also provides information on how to use the page and the different types of messages that could be displayed by the application. If the user is not able to resolve the issue, then there is a help desk number at the bottom, through which an incident record can be opened. Once the incident record is opened, it will be routed to the appropriate team to resolve the issue, based on the priority.

Here is a sample System Topology diagram.



Virtual Directory set-up

The ASP pages are placed in a physical folder. Using Internet Information Server (IIS) a virtual directory is created which should point to the physical folder. The authentication method should be set to “Windows Integrated Authentication”. All the Authenticated Users will have access to this page. Password information will be obtained from the user and an “xmlhttp post method” will be invoked to transmit the data from the client browser to the server. Since it is secure information, the transmission will be carried out through an https request, which uses Secure Socket Layer (SSL). The User-Interface is simple and self-explanatory for a password change.

COM+ components set-up

The business rules are implemented in COM+ server components, which are secured using COM+ security. The COM+ component will make calls to the back-end and update necessary information in the LDAP directory and audit database. The components are divided into Thin Business Object (TBO) and Business Object (BO). The TBO is responsible for authorizing the user's access to the application. The component is deployed as a Server Package. Security should be enabled at the application level and component level, which restricts the user access to the application. A role should be created. For example the role can be named as "Authorized Users" and the respective users/groups should be added to the role. Security is handled by COM+ which is referred as declarative security. The ObjectContext in COM+ has a property named as OriginalCaller, which identifies, who the calling user is and checks the COM+ role for authorization. The component runs under an identity (identity refers to Windows domain account) with least privileges. The BO performs the actual business validation and changes the password. The security for BO is set-up in such a way that it can be accessed only by TBO. It runs under a different identity. It can have only one role named "TBO User". The identity with which the TBO is running under should be part of the role of BO.

The Thin Business Object has COM+Client component. The Business Object has three components. They are ProcessManager, ProcessRead and ProcessWrite. Whenever a request is made, the ProcessManager evaluates the type of request and instantiates read/write components respectively. If a request is made to retrieve user information, the components binds the request with LDAP directory using the user credentials and then retrieves the user information. If a request is made to change the password, an LDAP bind is made to verify the authentication process and the password attribute is changed to the new value.

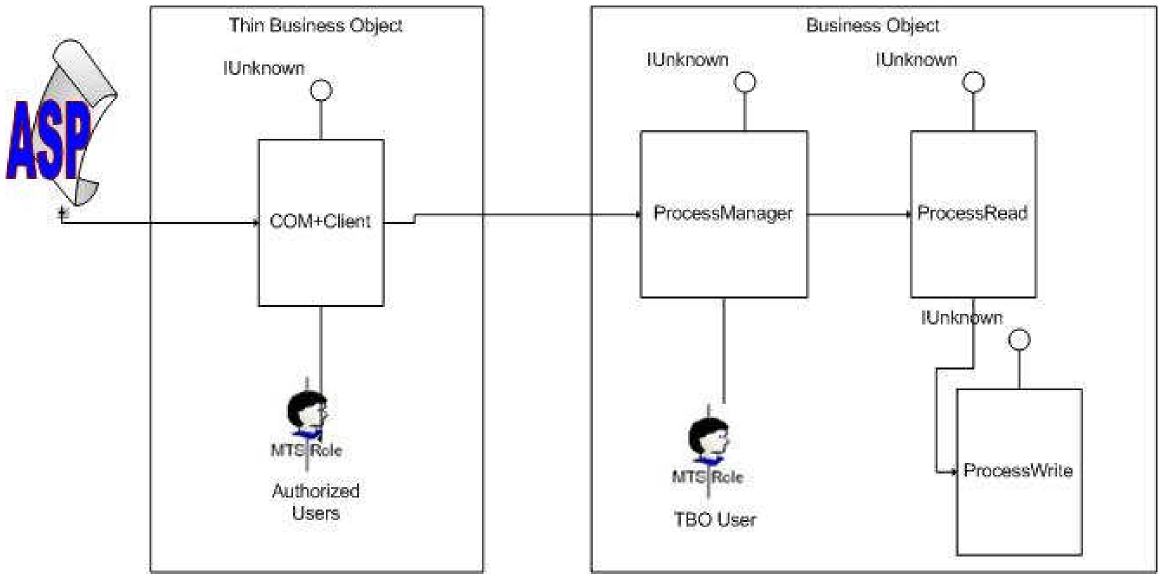
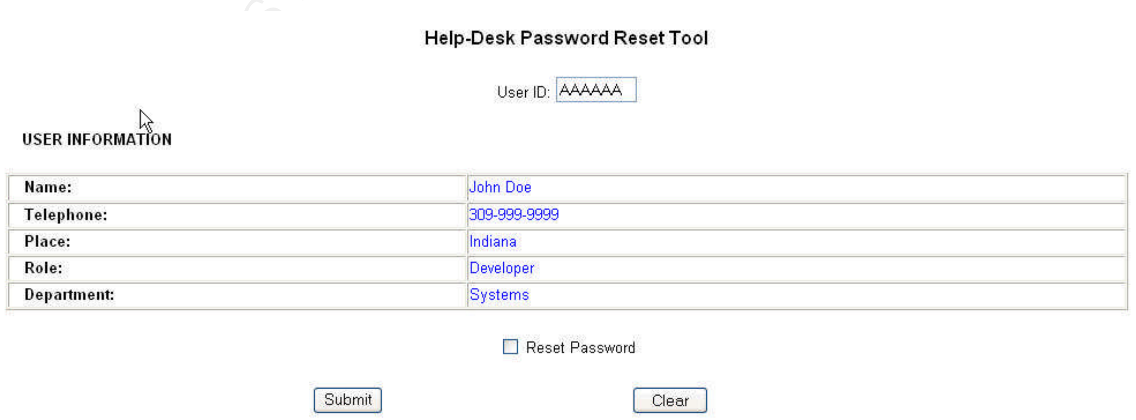


Figure 2: COM+ Role Model - Self Service tool

C. Help-Desk tool managed by administrators to reset user's password

The Help-Desk tool is developed to reset user's password. If a user forgets the password, the administrator can reset the user's password. Only the administrators will have the authority to perform this action. The administrators will be able to view the user information or reset user's password. This tool has a two step process. Once the user's id is keyed in and after the administrator submits the request, the system will retrieve user information, which will be used by the administrator to verify the user's identity. After verifying the identity of the user the administrator makes a request to reset the user's password. The credentials are passed to the LDAP directory for resetting the password. The system sets it to a default password and the user's password will also be expired, which enforces the user to change the password during the next login. Here is the sample user interface diagram.



The tool provides two different options:

- View the user information
- View/Reset user's password.

Certain administrators will have the ability to read the user's information, whereas other administrators will have the ability to view and reset user's password.

This tool will also follow the architectural pattern as mentioned in the previous tool. Authorization to the tool is controlled by COM+ Role Based Access control (RBAC) security mechanism. This application uses Programmatic security as it validates the user's presence in two different roles. One of the methods of COM+ ObjectContext is IsCallerInRole, which expects the role name to be passed as the parameter and it returns a flag true or false. If it returns true, then it indicates that the user is authorized to perform the appropriate operation, otherwise, the system sends a message back to the client stating that the user is not authorized. In order to evaluate this, the following access checks should be turned on in COM+ settings.

1. Enforce access checks for this application.
2. Enforce component level access checks.

There are two roles created namely QueryAdministrators and Query-ResetAdministrators. Those who are part of the QueryAdministrators role will have the ability to view the user information along with the password expiration status, whereas Query-ResetAdministrators will be able to view and reset user's password. Delegation of Authority to reset password can be handled very easily by developing tools, rather than providing administrative access to the entire system. Here is the diagram that depicts the COM+ role model.

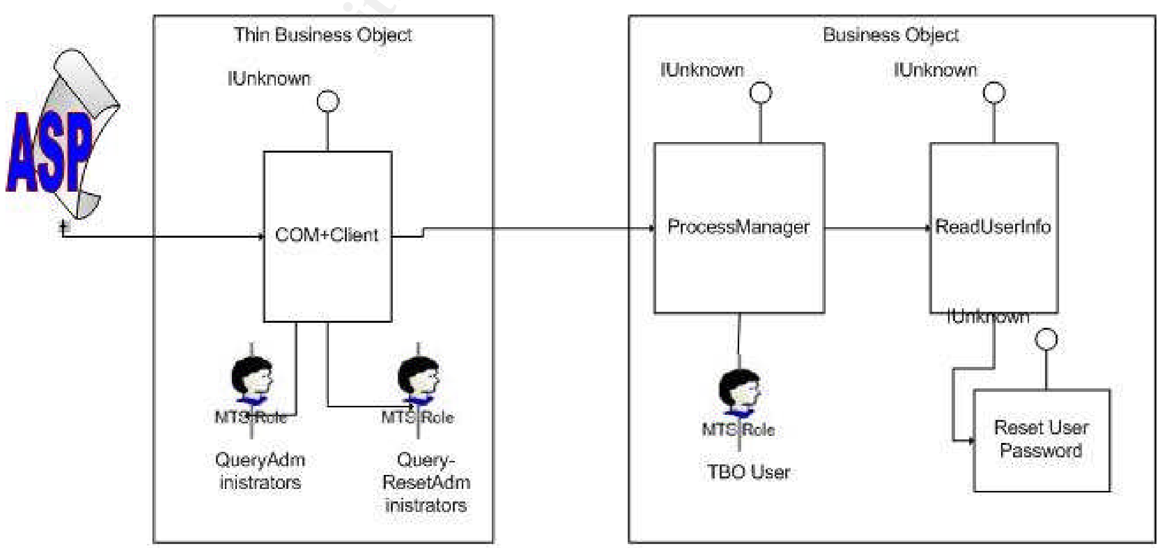


Figure 3: COM+ Role Model - Help-Desk tool

Application Auditing

Application auditing plays a vital role in forensics. The system adds an entry into the audit table for every transaction. It lists the date, time, user (for whom the password was reset), and administrator (the person who resets the password). A report can be generated from the table to identify the number of resets, which helps the organization in computing the Business Volume Metrics.

D. Self-Service tool for Password Reset

Using the technological advantages, it is possible to provide the most economical automated solution for password reset. On an average 25% to 30% of the calls are for password reset in an organization. The enterprise can overcome this by introducing a Self-Service tool for Password Reset through Voice Authentication. The user will have to go through a process to register their voice. The voice print will be stored in a database for future validation. After the registration process is successful, the user will be able to access the toll-free number and select the option to reset their password.

Cost Benefit Analysis

A sample cost benefit analysis is shown here. There are 2500 password resets handled by Help-Desk per business day at an average cost of $25 per call. An automated solution would cost $5 per call (net savings of $20 per call). Voice authentication is a requirement to the automated system. At an 80% success rate, that would translate to an annual savings of $9,600,000 approximately.

Intangible benefits

This system is secure. The success rate will be high. System is easier to use.

System Process for password reset through Voice Authentication

The automated processes include the following:

- Generation of mass email for the registration process.
- Voice registration process.
- E-mail to new Employees asking them to perform the voice registration.
- Password reset process for all employees.
- E-mail after successful password reset.

Mass E-mail Generation

An application is developed to generate and send mass e-mail to all users. The application components have the business rules incorporated and therefore the e-mails will be sent based on a roll-out schedule. This will be one of the batch processes, scheduled to run in the night.

Voice Registration

Another application is developed to carry-out the registration process. The users will be provided a provided with the instruction on how to register their voice print. The user will be expected to speak some numbers and words a few times, through which a voice print will be generated. On successful completion of the voice registration, an e-mail will be sent as a confirmation.

E-mail to New Employees

A batch process is created to send e-mails to new employees asking them to perform the voice registration. This application will also run in the night.

Password Reset & E-mail confirmation

A full-blown application is developed for password reset and to send e-mail after successful reset. When a user makes a call through phone for a password reset, the request is sent to Voice Recognition Unit (VRU) through PBX. The VRU runs on a UNIX server. The system requests the user to speak some words provided by the system. The system verifies the voice print against the information that is stored in the database. Once the voice print verification is successful, the request is passed to a Web Server through Hyper Text Transfer Protocol (HTTPS).   The request is handled by an ASP page, which re-directs the request to a mid-tier COM component. The credential passed by the VRU system is authenticated by the Web Server. The mid-tier component that was developed for the Help-Desk tool is being reused. The mid-tier component resets the password and sends a message back to VRU, which is sent to the requester. There is no manual intervention in this process. On successful completion of the password reset an e-mail will be sent as a confirmation for this request.

Here is the system topology diagram.

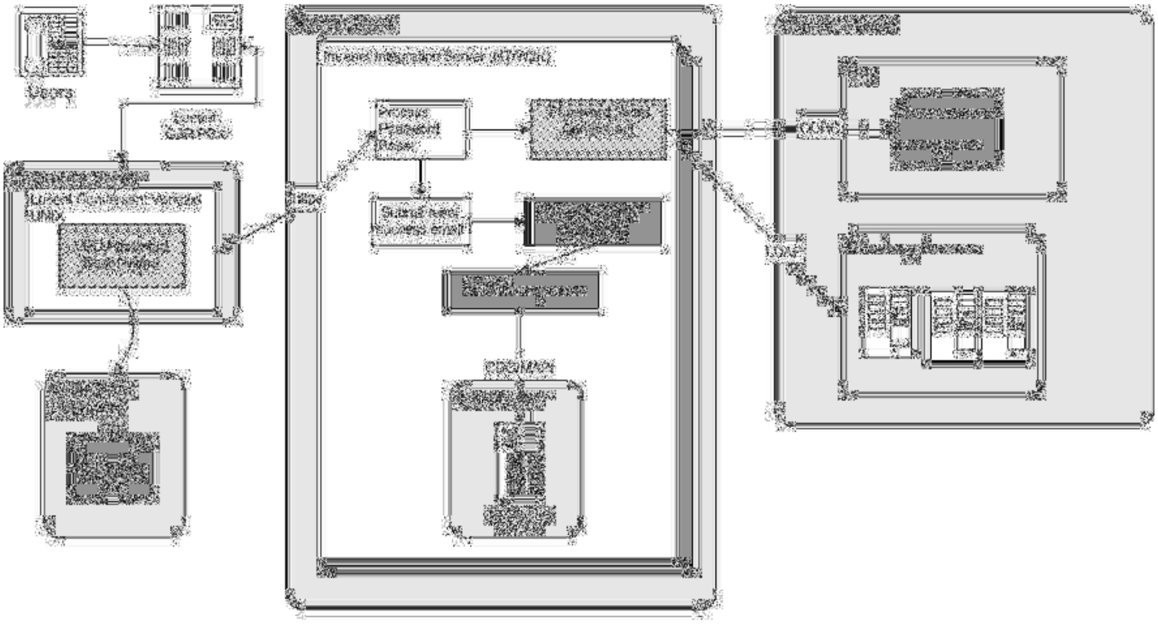


Fig 4:Password Reset thru Voice Recognition Unit

If the actual user did not make the request then, the user will contact the appropriate authorities to initiate an enquiry process. This implies that, this is a secure/fool-proof mechanism that could be adopted for password reset. This will help the user to make sure, whether a request was made by him/her. The password reset information is stored in the Audit Log table, which is used for analyzing the amount of usage and success rate etc. The system failures are properly accounted and error logging will be handled by host and mid-tier at the respective layers. This is mainly focused on medium and large scale organizations.

Conclusion

On the whole, this paper has explained the significance of Password Management and how it can be handled through various tools. The above tools were successfully implemented in production. There are several tools discussed in this paper, which could be used as a basis for building an enterprise solution for Password Management. The pros and cons of the various tools are also highlighted. With the evolution of technology, it seems that these solutions are highly conducive for different types of organizations. The tools developed are secure, easy to use, and cost beneficial, which is the key goal of every enterprise.

References

“Password Management Challenge.” Touchpaper.

URL:
http://www.touchpaper.com/uploaded_images/placeholders/passme_new.pdf
(29 June 2004).

"Password Management." Critical Path. April 2003.
URL:http://www.cp.net/pdf/sb-passwordManagement.pdf (29 June 2004).

Taylor, Steve. "Information Security Management." University of Auckland. 19 September 2003.
URL:
http://www.auckland.ac.nz/security/AccountAndPasswordManagementPolicy.htm
(29 June 2004).

"SecureLogin Single Sign-On Overview." Protocom Development Systems.
URL:
http://www.protocom.com/html/securelogin_single_sign_on.html?source=ggl_passwordmanagement (29 June 2004).

"Password Management Best Practices." M-TECH Identity Management Solutions.
URL: http://www.psynch.com/docs/best_practices.html
(29 June 2004).

Last Updated: May 29th, 2017

Upcoming Training

SANS Houston 2017	**Houston, TX**	**Jun 05, 2017 - Jun 10, 2017**	**Live Event**
Security Operations Center Summit & Training	**Washington, DC**	**Jun 05, 2017 - Jun 12, 2017**	**Live Event**
Community SANS Ottawa SEC401	**Ottawa, ON**	**Jun 05, 2017 - Jun 10, 2017**	**Community SANS**
SANS San Francisco Summer 2017	**San Francisco, CA**	**Jun 05, 2017 - Jun 10, 2017**	**Live Event**
SANS Charlotte 2017	**Charlotte, NC**	**Jun 12, 2017 - Jun 17, 2017**	**Live Event**
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	**Denver, CO**	**Jun 12, 2017 - Jun 17, 2017**	**vLive**
SANS Secure Europe 2017	**Amsterdam, Netherlands**	**Jun 12, 2017 - Jun 20, 2017**	**Live Event**
Community SANS Portland SEC401	**Portland, OR**	**Jun 12, 2017 - Jun 17, 2017**	**Community SANS**
SANS Rocky Mountain 2017	**Denver, CO**	**Jun 12, 2017 - Jun 17, 2017**	**Live Event**
SANS Minneapolis 2017	**Minneapolis, MN**	**Jun 19, 2017 - Jun 24, 2017**	**Live Event**
SANS Paris 2017	**Paris, France**	**Jun 26, 2017 - Jul 01, 2017**	**Live Event**
SANS Columbia, MD 2017	**Columbia, MD**	**Jun 26, 2017 - Jul 01, 2017**	**Live Event**
SANS Cyber Defence Canberra 2017	**Canberra, Australia**	**Jun 26, 2017 - Jul 08, 2017**	**Live Event**
SANS London July 2017	**London, United Kingdom**	**Jul 03, 2017 - Jul 08, 2017**	**Live Event**
Cyber Defence Japan 2017	**Tokyo, Japan**	**Jul 05, 2017 - Jul 15, 2017**	**Live Event**
SANS Cyber Defence Singapore 2017	**Singapore, Singapore**	**Jul 10, 2017 - Jul 15, 2017**	**Live Event**
Community SANS Minneapolis SEC401	**Minneapolis, MN**	**Jul 10, 2017 - Jul 15, 2017**	**Community SANS**
SANS Los Angeles - Long Beach 2017	**Long Beach, CA**	**Jul 10, 2017 - Jul 15, 2017**	**Live Event**
Community SANS Phoenix SEC401	**Phoenix, AZ**	**Jul 10, 2017 - Jul 15, 2017**	**Community SANS**
SANS Munich Summer 2017	**Munich, Germany**	**Jul 10, 2017 - Jul 15, 2017**	**Live Event**
Mentor Session - SEC401	**Ventura, CA**	**Jul 12, 2017 - Sep 13, 2017**	**Mentor**
Mentor Session - SEC401	**Macon, GA**	**Jul 12, 2017 - Aug 23, 2017**	**Mentor**
Community SANS Colorado Springs SEC401	**Colorado Springs, CO**	**Jul 17, 2017 - Jul 22, 2017**	**Community SANS**
Community SANS Atlanta SEC401	**Atlanta, GA**	**Jul 17, 2017 - Jul 22, 2017**	**Community SANS**
SANSFIRE 2017	**Washington, DC**	**Jul 22, 2017 - Jul 29, 2017**	**Live Event**
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	**Washington, DC**	**Jul 24, 2017 - Jul 29, 2017**	**vLive**
Community SANS Charleston SEC401	**Charleston, SC**	**Jul 24, 2017 - Jul 29, 2017**	**Community SANS**
Community SANS Fort Lauderdale SEC401	**Fort Lauderdale, FL**	**Jul 31, 2017 - Aug 05, 2017**	**Community SANS**
SANS San Antonio 2017	**San Antonio, TX**	**Aug 06, 2017 - Aug 11, 2017**	**Live Event**
SANS Prague 2017	**Prague, Czech Republic**	**Aug 07, 2017 - Aug 12, 2017**	**Live Event**
SANS Boston 2017	**Boston, MA**	**Aug 07, 2017 - Aug 12, 2017**	**Live Event**