Abstract—In corporate world, it is really tedious job to remember passwords of so many different systems. Many a times, users write their passwords on sticky notes just because of the fear of forgetting password. Or they tend to keep password very simple so that they can easily remember it. This is a major security loophole because such passwords can easily be guessed and hacked. Providing a fallback authentication mechanism, which helps the user to reset his password and unlock his account without calling the helpdesk, will eliminate those wasted minutes and dollars too. If a fallback authentication mechanism is provided to users to reset their passwords on their own instantly, from their own desktop and even without login to the system, this will address the problem from root.

Index Terms—Fallback Authentication, (Graphical Identification and Authentication, Automated password reset through E-Mail Authentication Service.

I. INTRODUCTION

It happens many times! A user tries to log into a corporate network but fails to remember his or her Windows password when prompted and is locked out of everything. As organizations adopt increasingly tougher security standards, today’s users are required to remember more passwords for more systems. These passwords are more complex and have a shorter lifetime than ever before. The increased likelihood of errors in recalling passwords generates an increase in calls to the Helpdesk for password resets. Overall, this decreases the productivity of the user. This is affecting the bottom-line of the business. [1]

Password management is the most common IT support issue bringing the most help desk workload in many organizations. Password complexity and expiration policy requirements lead to frequently forgotten passwords and account lockouts, increasing the overall administrative burden.

Manuscript received Dec 01, 2011.
Akhil Khare Department of Information Technology, Bharati Vidyapeeth Deemed University, College Of Engineering, Pune-46 (e-mail:Khareakhil@gamil.com).
Archana Burujwale Department of Information Technology, Bharati Vidyapeeth Deemed University, College Of Engineering, Pune-46

Fallback Authentication Manager should automate the process of resetting passwords. This will reduce the help desk calls and hence will increase the productivity and reduce the cost. So the Ultimate Goal - Low cost, higher productivity at highest security.

Automating process of resetting password involves –
a) Minimum footprint and no dependency upon any third-party software already being installed.
b) Modifying Windows authentication mechanism to launch Client Application for resetting password.
c) Develop Client Application which will communicate with Authentication WCF Service.
d) Develop Authentication WCF Service which will communicate with Database server (SQL Server 2005) for secondary Authentication and Reset Passwords on various Systems.
e) Develop a Configuration Manager Web Application which will allow user to configure Challenges/Responses.

Fig. 1: System Architecture

Above figure shows the different client workstation (where Fallback Authentication Manager’s Client Application is installed) communicating to the Authentication Service over HTTP for Challenge-Response authentication and password reset. End user will use his/her current desktop without actually logging into the system to use the reset password functionality. Authentication Service communicates with the Database server for Challenge Response Authentication and if authentication succeeds, Reset Password screen will be presented to the user and s/he can reset domain password.
II. PROBLEM DEFINITION

As organizations adopt increasingly tougher security standards, today’s users are required to remember more passwords for more systems. These passwords are more complex and have a shorter lifetime than ever before. The increased likelihood of errors in recalling passwords generates an increase in calls to the Helpdesk for password resets. Overall, this decreases the productivity of the user. This is affecting the bottom-line of the business.

Password management is the most common IT support issue bringing the most helpdesk workload in many organizations. Password complexity and expiration policy requirements lead to frequently forgotten passwords and account lockouts, increasing the overall administrative burden. [1]

Consider an organization having thousands of employees having individual workstations. As per a study, in such a big environment, as much as 30 percent of all helpdesk calls are password-reset requests, on average every request takes 20 minutes to resolve and costs more than $23 on helpdesk operations alone, says market research firm Gartner.

In corporate world, it is really tedious job to remember passwords of so many different systems. Many a times, users write their passwords on sticky notes just because of the fear of forgetting password. Or they tend to keep password very simple so that they can easily remember it. This is a major security loophole because such passwords can easily be guessed and hacked.

There are various alternative trends for resetting password of an employee in an organization in case s/he forgets his/her password.[1] Here are most widely used alternatives –

A. Help-Desk call

The most commonly used way to reset the password of an employee is to call a help desk executive and provide user name and answer few questions on the call. If the executive is convinced about your identity, s/he will reset the password for the employee.

The major drawback of such a system is, it is less secure and involves high cost.

B. Automated password reset through E-Mail

In such a system, user needs to submit a password reset request through a web application and the system will reset a randomly generated password and sends it in an email to user’s configured email account.

The limitation of this system is user needs to access the help desk website and his email account for which he requires another workstation.

C. Password reset web application hosted in intranet

This kind of solution has a web application where user needs to enter other credentials to login and then the application allows user to change his domain password.

Limitation of such solution is to access the web application, user needs a computer, as he is unable to login to his computer, he has to disturb his colleague to get access to the system. Also this requires user to remember other set of credentials through which he can login to the web application.

D. A dedicated workstation for resetting password

In this system, the organization dedicates the workstation for resetting password in case an employee forgets his/her password. The dedicated workstation has common password which is known to every employee. By accessing the workstation the employee can access the helpdesk website to reset his/her password.

The limitation of such a system is, in case the reset password workload is high on a particular day (say after Holidays) the dedicated workstation becomes the bottleneck.

III. TECHNICAL SPECIFICATION

A. GINA (Graphical Identification aNd Authentication)

This component, developed in C++, will get invoked by windows operating system. This in turn will invoke windows default authentication mechanism. In addition this component will add “reset password” button on windows log in screen.

As per Microsoft documentation, “[GINA] Graphical Identification and Authentication component that serves as the gateway for interactive logons. GINA is the pluggable part of WinLogon that third parties may replace in order to customize the functionality or the UI of the logon experience in Windows. By replacing GINA, one can choose the authentication mechanism Windows will use for interactive users. This is often useful for smartcard or biometric logons or hooking some other authentication mechanism.

GINA collects credentials from local and remote users (the latter via Terminal Services) who want to establish an interactive logon on the machine. It then establishes a logon session for that user. If GINA were compromised, it could be used to steal plaintext user passwords, user biometric data, smartcard PIN codes, and so on. A compromised GINA could act as a back door, letting a certain normal user log in with administrative privileges. GINA component runs as SYSTEM, accepts input from local and remote users, and runs all the time.”[4]
To deploy the GINA, the installer program will copy the DLL onto the target machine in the System32 directory, and update the machine's registry by adding a named value under WinLogon's key: HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\WinLogon

The named value should be GinaDLL, of type REG_SZ, and its value should be the name of the DLL. A reboot of the machine is required to complete the installation.

B. Credential Provider

The Windows logon process (winlogon.exe) has been completely re-architected in Windows Vista. One core requirement of that effort was to move plug-ins out of the winlogon process space to the fullest extent possible. That requirement was born of reliability concerns. If, for example, a poorly written GINA is loaded into the winlogon.exe instance running in session zero on a server, a software fault could kill that critical process and in turn the machine itself. And even if GINA could have been adapted to run out of process, there would still be the issue that it wasn't designed to provide a consistent, controlled experience across arbitrarily complex, interactive credential-gathering scenarios.

So, in Windows Vista, the Graphical Identification and Authentication (GINA) credential input extension model has been deprecated in favor of a more robust, stable and straightforward credential provider model. Previously, there could only be one GINA on a system, which sometimes made deployment difficult and limited the flexibility of the system. Windows Vista now enables you to have multiple providers. To add a provider, we need to register that COM object and also make an entry into registry at HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers\location. LogonUI enumerates all of the credential providers registered under this location.[5]

In Windows Vista,GINAs are replaced with a new modular Credential Provider model that is easier to program to. Credential Security Service Provider (CredSSP) is a new security service provider that is available through the Security Support Provider Interface (SSPI) in Windows. The Credential Provider, COM-based architecture, requires each provider to enumerate its UI elements. For example, in a given scenario, a provider might indicate to LogonUI that it requires two edit boxes, two captions, a checkbox, and a bitmap. In turn, LogonUI renders those controls on behalf of the credential provider.

Hence Credential providers are the Plug-Ins to LogonUI. LogonUI can interact simultaneously with multiple credential providers. Above figure illustrates WinLogon Architecture.

Above figure elaborates more on the execution of the new mechanism. First, the console session LogonUI process is started by winlogon. Upon creation, LogonUI enumerates all of the credential providers registered under HKLM\Software\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers\location. LogonUI enumerates all of the credential providers registered under this location.[5]
The valu CPGSR\_RETURN\_CREDENTIAL\_FINISHED makes this distinction. After GetSerialization, LogonUI passes the marshaled credential to winlogon, which in turn passes it to the Local Security Authority (LSA) by calling LogonUser. Prior to this, LogonUI calls Credential::UnAdvise and Provider::UnAdvise to notify both entities that notifications on their respective Events interfaces are not being accepted. UI changes would be pointless with a logon attempt pending (ideally, the next thing the user sees is his desktop).

Fig. 5 Functional working of customized Credential Provider

To provide facility to change password using challenge / Response mechanism, a Credential Provider will be added to the system. This Credential Provider will have one tile called “Forgot Password?” LogonUI calls Credential::SetSelected when the tile is selected. In this function the Client Application will be launched which will perform the challenge / response operation and reset the password if the responses are correct. When the dialog exits, the function Credential::SetSelected returns false to indicate that we need not to go further and the user again sees the enumerated tiles of LogonUI.

C. Client Application

This desktop application developed in C#.NET will facilitate user to answer configured questions and will also allow user to reset his/her password. For pre - Windows Vista Operating Systems, GINA DLL will be responsible to invoke this application while in Windows Vista onwards Operating Systems Credential Provider will be responsible for invoking this application.

Below screens illustrate the Client Application’s GUI for different steps of fallback authentication.

D. Authentication Service

This .NET WCF service will be responsible for authenticating user using challenge response mechanism and if user succeeds in answering configured questions correctly then this will enable user to reset the password. This service will then propagate the new password of the user on various configured systems.

Below figure shows the communication that will happen between Authentication Service and the Client Application.

E. Configuration Manager

This is an ASP.NET (C#) web application which will provide two important functionalities.

From this web application, user can configure challenge responses. The challenges and responses will be stored in the database. The Client Application will prompt for these challenges when executed.

In addition, this application will facilitate the user to map his user name with his various accounts on various different systems in the organization. This configuration will be used by the Authentication Service to propagate the new password on various systems.
F. Basics of WCF Service

WCF is a runtime and a set of APIs for creating systems that send messages between services and clients. The same infrastructure and APIs are used to create applications that communicate with other applications on the same computer system or on a system that resides in another company and is accessed over the Internet.

IV. CONCLUSION

Fallback Authentication Manager provides self-service to users to reset their passwords on their own in few minutes even before login to the system and propagate it to various systems. This SYSTEM requires modifying the Operating System’s authentication mechanism and hence will be a good learning experience. Also from usability perspective, this project will help avoiding – High call volume: Users forget or lock out their passwords. This can be 30% of help desk workload, Sticky notes: Users write down their passwords and may leave them in public view, Bad passwords: Users choose simple, easily guessed passwords, Loss of productivity when users are having logging trouble, Overhead helpdesk staffing for peak volumes after holidays.

REFERENCES


AUTHOR’S PROFILE

Mr. Akhil Khare is working as an Associate Professor in Information Technology Department at Bharati Vidyapeeth Deemed University College of Engineering, Dhankawadi, Pune India. He was awarded his Master of Technology Degree from RGTU Bhopal. His areas of interest are Computer Network, Software Engineering and Multimedia System. He has nine years experience in teaching and research. He has published more than twenty research papers in journals and conferences. He has also guided ten postgraduate students.

Archana Burujwale from Information Technology Department at Bharati Vidyapeeth Deemed University College of Engineering, Dhankawadi, Pune India. Her areas of interest are Software Engineering and Multimedia System. She has Five years experience in teaching and research.