



Your Information Security Ally™

Managing Embedded Application Passwords with Password Auto Repository™ (PAR)

[WHITE PAPER]

Written by
e-DMZ Security, LLC

February, 2007

Managing Embedded Application Passwords with Password Auto Repository (PAR)

Introduction:

Password management has long been a key security and compliance focus for today's enterprise. From an initial focus on user password management to more recent attention on the more difficult challenge of shared account password management (SAPM), the issue of password management continues to create regulatory, compliance and security concerns for the enterprise.

One area often overlooked in the discussion of enterprise password management is embedded application passwords. Since the move from a centralized to distributed computing and networking model, applications of all types have had the requirement to communicate with other applications, systems and devices. In many cases this communication required the application to "login" and/or "authenticate" through a specific account/password. With no other method available, the required information was hard coded into the application.

Today many enterprises have hundreds or even thousands of applications using embedded passwords for application to application (A2A) and application to system (A2S) communication. Do you know how many applications have hard coded passwords in your enterprise? Because these passwords are hard coded, they are rarely if ever changed and as a result become overlooked by the enterprise. However, they are known by various application programmers and can provide a "back-door" into your applications and systems. In many cases this access is at a privileged level!

Growing regulatory and compliance audits are bringing the issue of embedded application passwords to the forefront of password management. Though it may seem a daunting issue to solve, there is a solution that not only eliminates the need for embedded and hard coded passwords, it provides automated release controls, change controls and audits to meet the most demanding regulatory and compliance needs. The solution is e-DMZ Security's Password Auto Repository (PAR).

A new solution to an old problem:

Password Auto Repository (PAR) was designed to solve the security, regulatory and compliance issues associated with the management and control of shared account, service account and embedded passwords. From SME to some of the world's largest enterprises, PAR is deployed and proven in meeting these unique password management requirements.

The management of embedded and hard coded A2A and A2S passwords is met by PAR through the advanced Command Line Interface (CLI) and Application Programmers Interface (API).

PAR CLI Overview

The PAR CLI provides a method for properly authorized applications or automated processes to retrieve information from PAR or perform limited actions to the PAR. Through the CLI, the enterprise can replace existing hard coded passwords with specific and secure commands to PAR to retrieve the required password. The back-end change control features of PAR can be configured to assure the password is changed based on enterprise specific requirements. The use of the CLI is secured as follows:

1. CLI commands can only be executed by configured “CLI Users”
2. CLI uses SSH force commands to assure only authorized PAR CLI commands are executed
3. CLI connects to PAR via SSH using DSS key pairs
4. Source restrict by IP allowing usage only from specific hosts

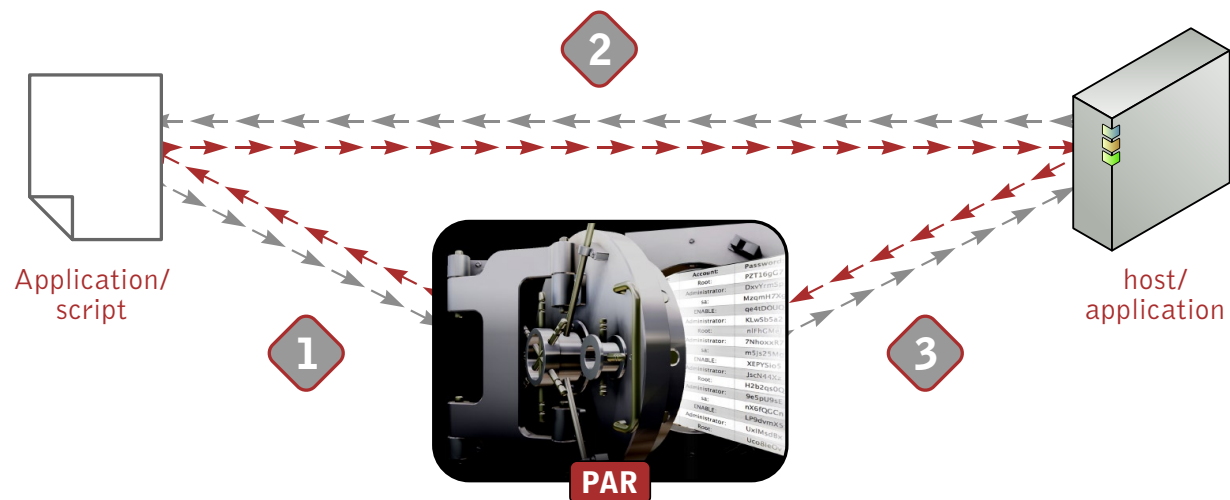
CLI commands can be executed as part of a script or via appropriate exec() application calls.

A typical CLI password retrieve command would look as follows:

ssh -I cliuser1.181.txt.Cliuser1@192.168.0.161 Retrieve alin10a, root,8, application xyz access

In this example, the root password for system alin10a would be retrieved. PAR would audit this access from Cliuser1 including the reason for access, in this case “application xyz access”.

Looking at a high level logical flow diagram as shown below, you can see the flow and interaction between the application, PAR and host/application.



1. Application or script retrieves required password from PAR
2. Application connects to required host/application using password obtained from PAR
3. Through PAR change controls, PAR can change account password as required by enterprise policy

The robust commands available through the PAR CLI allow its use to extend beyond replacement of existing hard coded and embedded passwords to include the development of automated scripts and programs to drive a host of functions including:

- PAR user management
- PAR system management
- System account management
- Password retrieve, test, change
- Password verification and synchronization

PAR API Overview

With release 2.0, PAR includes a robust API to compliment our CLI for those programming environments that require PAR command access from within complied applications. Like the CLI, the PAR API supports a rich set of PAR commands to support the replacement of embedded and/or hard coded passwords. PAR functions available through the API include:

- PAR user management
- PAR system management
- System account management
- Password retrieve, test, change
- Password verification and synchronization
- File retrieval

As with the CLI, the PAR API will logically connect as is reflected in Diagram 1. The API will target support for many of the most common development environments including:

- PERL
- C/C++
- Visual Basic
- Java

The communication between the calling application and PAR will be secured via SSH using DSS key pairs thus assuring both communication security and connection integrity between the application and PAR.

Additional A2A and A2S Values and Features

- Using PAR system based licensing, there is NO ADDITIONAL COST for using PAR to replace your embedded or hard coded passwords with CLI and/or API based password retrieval.
- PAR is completely clientless. PAR does not require client/host software – reducing deployment complexity and life cycle support costs.
- PAR is an appliance based solution – there are no hidden or additional 3rd party hardware or software requirements.



Your Information Security Ally™

501 Silverside Road • Suite 143 • Wilmington, DE 19809

Phone: 302.791.9370 • Toll Free: 866.203.9823 • Fax: 302.793.4985