



Password Auto-Repository™ (PAR) Security Overview Whitepaper

Version 2.0
Last Updated 6/1/2008



Architecture

The Password Auto Repository™ (PAR) is designed to provide a secure method for storage, management, changing, and release of administrative passwords. The focus is on shared accounts such as 'root' on Unix, 'Administrator' on Windows servers, and powerful administrative accounts on databases (Oracle, SQL Server, etc.). The PAR provides role based access control to provide dual control for the release of passwords. The interface to users and administrators is HTTPS, allowing for a clientless installation. Communication between the PAR and Unix based managed systems is via SSH, which can be further controlled using SSH capabilities, such as force commands and DSS keys.

Interfaces:

Configuration Interface - This interface is accessed via a direct crossover connection to a special dedicated configuration Ethernet port. This port is defined as non-routable (using a RFC1918 address) and cannot be changed. The requirement for physical access to the device is an additional security feature. The configuration interface is only needed for initial configuration of the PAR appliance (network settings), for restoring a PAR from an encrypted backup file, or for modifying the underlying security credentials such as the DSS private key or the X.509 certificate used for the password encryption process. For environments where physical access to the machine is not feasible, it is possible to configure access to this interface via authenticated HTTPS on port 8443 at the PAR network address.

Administrative Interface - The Administrative interface is accessed via an authenticated HTTPS connection through the primary PAR network interface. This interface is available over the network. It is accessed by administrative users only. The Administrative interface is used to define global PAR options, manage the automated backup process, control the High Availability settings, and configure internal processes such as the mail agent and the automation engine. The Administrative interface is also used to apply maintenance updates to the PAR. Configuration for external authentication services and PAR licensing is also managed through this interface.

User Interface - The PAR User Interface is the access method for interactive users of PAR. This interface is accessed via an authenticated HTTPS connection through the primary PAR interface. This interface is available over the network. Role based access control (RBAC) dictates the menu items that are displayed for each user. The global roles of Auditor, PAR User Administrator, and PAR Administrator are mutually exclusive, and provide global capabilities to the PAR instance. The roles of PAR Requestor, PAR Approver, PAR Approver/Requestor, and PAR ISA (Information Security Administrator) can be granularly assigned to each managed system. PAR ensures the permissions assigned, whether through groups, collection, systems, or users, do not violate the segregation of duties around the release of a managed account password.

Automation:

Auto Management Agent - This agent performs all background password management functions, including password checking, password changing, and the changing of service startup passwords on member servers that are dependent on a domain account changed by PAR. This is a multi-threaded agent that dynamically starts the appropriate threads based on the size of the queue for each of these tasks and tuning preferences set by the

PAR system administrator. The check process provides the validation on the managed system by establishing a session with the managed system, and compares the credential stored within PAR against the value on the managed system. If a mismatch is detected, PAR notes this in the audit trail and schedules a Password Change for the account. The Password Change process consults the password construction rule for the managed account and then generates, encrypts, and stores the new password within PAR. The Password change agent then establishes a connection with the managed system and attempts to change the managed account. For scale, up to 10 automation processes can run concurrently on PAR and up to 100 on the Enterprise PAR (EPAR).

PAR Mail Agent- The PAR mail agent is responsible for sending email messages from PAR. PAR will attempt to send mail to notify PAR Approvers when a Password Request has been submitted requiring their approval, as well as notifying the PAR Requestor when the request has been approved. The PAR mail agent also sends notification based on abnormal events, such as a managed system becoming unavailable, or loss of connectivity to the PAR High Availability (HA) Replica.

PAR Replication Agent- The PAR Replication agent maintains the consistency between the PAR Primary and the PAR Replica in a High Availability pair. The PAR replication agent utilizes the IPsec tunnel between the PAR partners to ensure the confidentiality of the information.

Security Review

Network Security

Users connect to the PAR using HTTPS. This protects the confidentiality of any passwords or data between the user and PAR. The users authenticate to PAR using integrated Windows authentication, where the password parameters are set to enforce strong password construction, aging, and history. In addition, external authentication can be required on a user by user basis. External authentication currently supports SecurID™ (RSA®), Safeword™ (Secure Computing®), LDAP(s), Radius, and Windows Active Directory..

The PAR is protected via an embedded CyberGuard® SG640 Firewall. This Firewall is configured with the following rules:

- HTTPS (443/tcp) is permitted inbound to PAR
 - Optional HTTPS over port 8443 may be user enabled
- SSH2 (22/tcp) is permitted inbound to PAR for CLI access
- Connections from the PAR and their responses are permitted
- Other traffic directed to the PAR is dropped

In addition, PAR provides the ability to send an SMTP alert if a threshold of invalid packets directed to PAR is detected. All information from the embedded firewall is logged to the PAR and is available through the PAR reporting interface.

The Web server is secured in accordance with Microsoft's guidelines for IIS security. The appliance is hardened such that unnecessary services are disabled, even though the firewall assures that these services are unavailable.

Access to the firewall configuration is not permitted, instead it is changed automatically only as necessary when changes are made to the PAR network settings from the configuration interface.

Encryption and Key Management

The encryption for the HTTPS is standard SSLv3. The initial certificate used to provide the server authentication is a certificate signed by e-DMZ Security's CA. From the configuration interface, customers can and are suggested to replace this initial certificate with a specific certificate signed by a CA trusted in your environment. This improves security and tremendously improves performance of the application interface.

The encryption for the SSH2 connections is AES256. The keys for this encryption are negotiated for each connection with authentication provided via the DSS asymmetric keys. The PAR can generate its own DSS key pair, only exporting the public key. The private key is included in the encrypted back-up, making this a very secure option. If an existing keypair is desired, PAR also allows the import of an external DSS private key. The DSS private key is modified through the configuration interface. PAR also permits the use of a unique key for each system under management. In this case, the key is generated or re-generated on the definition page for each system.

The encryption for the Password storage is AES256 authenticated via an installed X.509 certificate. The encryption is provided by an off the shelf product that is integrated with the RSA BSAFE toolkit.

Command Line Interface (CLI) and Application Programming Interface (API)

The available CLI and API access to PAR uses SSH2 connections to PAR from authorized clients only, authorized by a public/private key pair. Each CLI/API ID created holds a separate key pair. Additionally, the CLI/API access uses Force commands to ensure that only specifically allowed commands may be executed by authorized CLI/API IDs.

Database Security

The communication between the Web application and the database are secured by only allowing stored procedures to be called from the application. No ad-hoc SQL is allowed, which greatly reduces the chance of malformed URLs allowing unanticipated behavior. In addition, authentication checks are done on each stored procedure call to ensure that previously accessed information can not be retrieved without current authentication credentials.

Application Security

Segregation of duties is enforced through the Role Based Access Control (RBAC) designed into the application. It ensures that a single ID can not have conflicting roles for a managed system. This means that the application will not allow a single ID to have both approver and requester permissions for a managed account, even if the combination of Groups, Collections, Users, and Hosts would make this occur.

In addition, the application authentication is passed through to the underlying database via Windows integrated authentication. Once the user's role has been determined at the database, the application presents only the authorized menu choices.

Individual Accountability is enforced on Auto-Managed systems based on the application generating and updating the password on the managed system without any individual intervention. Only after a request is approved will the managed password be revealed.

Physical Security

The hard drive for the PAR is protected via full authenticated disk encryption (AES256) provided by Guardian Edge's Encryption Plus Hard Disk™. This ensures that even if the PAR is lost or stolen, the disk can not be accessed outside of the appliance. This prevents attempts to remotely mount the drive to bypass access controls.

Vulnerability Testing

After each major revision of PAR, it is scanned using the commonly available tools (ie. Nessus, NMAP, etc) to ensure that no high or medium risk vulnerabilities exist. Low risk vulnerabilities are evaluated to determine if they are required for proper functioning of the product. An example is that the IIS password change application will show as a vulnerability based on the ability of a remote user to try and brute force a password. This facility is needed to allow legitimate users to change their passwords. Since failed security events are logged and reported, this risk is mitigated but can not be eliminated without a more severe consequence (ie, Users not able to change their passwords periodically).

Audit Trail

All actions, whether administrative or user based, are recorded in PAR and are available for review. In addition, log information from the Firewall, Database, and Web Server are also available.

Appliance Access

All console access to the PAR is disabled. All routine maintenance activities are accomplished through the Administrative interface. This includes product and OS upgrades as well as reviewing diagnostic information.