

Password control

# Password Auto-Repository

**Supplier** e-DMZ Security LLC  
**Price** from \$12,000  
**Contact** www.e-dmzsecurity.com



There are many articles written about the need for robust passwords, and strong views are expressed on the ideal length and composition of a password, how often it should be changed and the kind of encryption schemes that should be used. This is an important subject, since there are several freely-available password-cracking programs that can make short work of decoding a weak password with a simple encryption scheme.

However, while it is obviously desirable to have strong passwords to protect key systems and services, the physical security of the passwords is often given less attention. There is little point in having a strong password if it is freely available to anyone who happens to pass by, either on a list pinned to a notice board or in a plain-text file stored on an insecure workstation.

There is very little that can be done to persuade users not to be so careless, but there is no excuse for system administrators doing it – and the consequences can be far more serious if a system administration account password falls into the wrong hands.

Most installations will have some kind of password-control mechanism in place, often involving passwords being kept in physically secure locations such as a lockbox or safe, and requiring at least one other person to be present when the password is removed and then returned after use. Passwords often need to be changed after use, with the new one being placed in the secure storage afterwards.

These procedures generally work well, although there can be problems when authorized personnel are unavailable. A more serious problem arises when a large number of systems need to be controlled and administered. The number of passwords required soon expands,

and the chances of duplicate passwords occurring across multiple systems are increased.

This is where a device such as the Password Auto Repository (PAR) comes into its own, with its ability to support a large number of systems.

Each system's password is stored in the PAR's encrypted file system, and can only be obtained by a user with an appropriate PAR account. The system will only release a password to an authorized user, and then only if the request is validated by an authorized approver.

An authorized approver does not have to be physically present to release the password, because all password release requests and approvals are carried out through a secure web connection with email notifications from the system itself.

A password's release permission can be limited to a specified time period, and all requests and approvals are logged for audit purposes. The PAR can be set up to change a password automatically after it has been used, which is in line with recommended procedures.

Rules can be set up to control how passwords are constructed for various systems and accounts, while global parameters deal with factors such as the time interval between password changes and the duration of account lockouts.

The system has extensive reporting facilities, providing logs of all changes made to the PAR's database, including the addition of new users and systems, lists of systems and accounts, and various user activity logs. The Password Update Activity report, which gives chronological details of all password changes, with reasons, would be of particular interest to security auditors. The system also provides a Test Agent service, which can be set to

check periodically that the passwords held on the remote systems match those held in the PAR.

The system, in a 1U rack-mountable chassis, uses a hardened version of Windows Server 2003, with an encrypted disk system. There is no redundant power supply, which is unusual in a mission-critical system, but the unit can operate in "High Availability" mode with a second PAR, which should provide the required resilience.

The system is normally administered from a workstation using a web browser and an encrypted network connection. Apart from configuring systems and accounts, the interface also gives access to system maintenance facilities, such as system updates and backup scheduling.

The PAR can operate with a range of operating systems, including HP-UX and AIX as well as Windows and Linux, and can support Sybase, Oracle and SQL Server database management systems.

Initial set-up requires the connection of a keyboard and monitor to release the encrypted disk system. Once this is done, all further system configuration can be carried out using a laptop or workstation connected to the system's dedicated configuration interface.

The system's built-in CyberGuard firewall, which is integrated into the network interface card, needs to be configured at this point, and the addressing details for the



High Availability option can also be set. The PAR can then be rebooted to apply the changes.

Here it becomes obvious that the disk encryption driver is still password-protected, and the keyboard and monitor must be reconnected before the system can be brought back up. This has system-recovery implications, since the PAR will not be able to restore itself automatically after a power supply interruption, planned or otherwise. The vendor tells us that a solution to this problem is being worked on.

Ian Parsons

SC MAGAZINE RATING

Features	★★★★☆
Ease of use	★★★★☆
Performance	★★★★☆
Documentation	★★★★☆
Support	★★★★☆
Value for money	★★★★☆
<b>OVERALL RATING</b>	<b>★★★★★</b>

**FOR** It can handle large numbers of systems in a standardized manner.

**AGAINST** It needs a terminal and keyboard attached whenever a reboot is needed.

**VERDICT** If you have a large number of system passwords to manage, this could be an effective solution.

Contact details:



e-DMZ Security, LLC

501 Silverside Road, Suite 143  
 Wilmington, DE 19809  
 (toll free) 1.866.203.9823  
 (fax) 302.793.4985

Email: par-info@e-dmzsecurity.com