



Zserver Works Fast

There seems to be virtually no end to the length an organization is willing to go in order to secure and protect their network perimeter from external attacks. From firewalls and intrusion detection systems, to stringent internal security policies, companies take external threats seriously and are relatively successful in shielding corporate data from external attackers. However, these perimeter security tools are often powerless against employee negligence or worse, malicious intent and actions.

Confidential data can easily fall into the wrong hands. The careless disposal of unsecured hard drives, back up tapes and other storage media is extremely damaging, yet even more harmful to a business can be breaches caused by a disgruntled IT employee. These employees' malevolent acts are extremely difficult to detect and uncover compared to external attacks. IT personnel have high-level or administrator access privileges, when coupled with their intimate knowledge of the network make internal threats far more likely and dangerous than any external breach.

Second only to erasing and locking hard drives and storage media in a safe, the most effective way to protect stored information is to encrypt it. Even when an unauthorized person gains possession of the storage media, without the encryption key, an enormous amount of computing resources are required to make any sense of and recover the data. Even if an individual has access to the government-level of computing power required to break an encrypted disc, the amount of processing time required to decipher the data can extend well beyond any reasonable and useable limits. Therefore, it's not surprising that a wide variety of data storage encryption solutions are on the market

PC Week recently evaluated one such product, the Zserver 5.0 trial edition, from leading Russian internal security company, Zecurion. Zserver 5.0 encrypts data stored on servers in real-time without producing a noticeable affect on running applications and overall network performance. The products notable features include:

- Secure storage of data access keys in password-protected files on removable media (flash drives, floppy disks etc.) and PIN-protected smart cards
- Data access key quorum where multiple access keys can be generated allowing the data to be read only with a combination of several keys. For example, if four data access keys are generated in total, access to the data is granted with any two of the keys in hand
- Local and remote administration. When working remotely, all communications are carried out over TCP/IP network protocol, with the data packet traffic being automatically encrypted in real-time
- Capability to send an "alarm" signal to block access to data, in case of emergency. The signal can be sent from a local or remote computer

- Support for MS Cluster Services
- Management of access to shared files, residing on the encrypted server partitions
- Support for calling script scenarios triggered by events, such as opening and closing of encrypted partitions, receiving “alarm” signal etc.
- Utilization of prominent encryption algorithms
- Encryption of data backups, such as streamers, SANs and CD/DVD drives

Zserver 5.0 is easy on network resources and requires only modest system assets such as, 128 MB of memory with a Pentium processor or higher. The Zserver server-side component (the encryption module) works with Windows Server 2000 SP4/Windows Server 2003 SP1. The management console and alarm module are compatible with Windows 2000 SP4 or later. In addition to the software installation, the basic package includes a USB license key, a smart card reader ACR ACS-30U, two smart cards ACOS1, as well as the system administration manual and installation instructions for the smart card module. The USB license key is used for validating the software licensing and storing the system configuration settings.

Zserver testing was conducted on an old server with dual processors mounted on TYAN Tiger i7505 motherboard, running two Intel Xeon CPUs (frequency of 3.06 GHz) with 2.5GB of RAM (DDR 2100). The operating system files and all other server software were installed on Samsung HD401LJ 400GB hard drive (primary disk) connected to the motherboard via a conventional SATA controller. The file encryption was performed on Maxtor 6Y160P0 160 GB hard drive mounted as a secondary disk, because by pure design; Zserver does not encrypt the operating system files

Zserver installed smoothly without any difficulties or special knowledge required. The supplied documentation gave enough detail for the system set up and was ready for operation by a typical experienced user. We did not however, have a chance to load the access keys from smart cards. Drivers for the smart card reader were properly installed, the Zserver-supplied utility had correctly identified the device, yet the main management console could not display the reader in its tree view. The problem was probably caused by the number and variety of programs installed on the server, potentially producing software conflicts. Running the tests on a “cleaner” machine was not technically feasible. As a result, saving and loading of keys was limited to an alternative data storage device, such as two flash memory sticks and two floppy disks. For purposes of the test, four access keys were generated with a quorum of any two required to access the data. The system supported several sources of random data gathering for generating the keys, including computer mouse movements and time intervals between receiving data packets from the local network

Initial encryption of the disk, with its storage capacity filled up to 80 percent, took approximately four and a half hours. During the operation, the computer was intentionally used for two other resource-intensive tasks, including continuous music playbacks (where the music files were stored on the disk partition being encrypted) and archiving large volumes of data (residing on both disks). As advertised by Zecurion, the initial disk encryption process and the subsequent use of the encrypted files did not cause any noticeable slowdowns in server performance.

Upon completion of the disk encryption, we conducted tests to determine if the computer's speed was impacted when working with encrypted files. The results showed only a slight decrease in the processing speed. When repeatedly copying a large file of 26 GB from an unencrypted data partition to the encrypted disk, the operation took 585 and 588 seconds respectively. The same operation between two unencrypted partitions took 576 and 581 seconds. The notable differentiation took place in CPU utilization, where we found substantial variation. During the normal copying operation (without the data encryption step), CPU utilization rates ranged between three percent and 18 percent, whereas transfer of data from unencrypted storage to the encrypted disk resulted in a minimum of 20 percent CPU usage, with typical CPU utilization between 35 percent to 45 percent, and peaking at 60 percent. We noticed that peaks and valleys of the CPU usage corresponded to the ending of the initial file copying and the beginning of the second copy. The increase in CPU usage did not visibly affect other ongoing activities, such as working with a text editor or compiling a large project

In addition to testing the basic functionality of encrypting data, we evaluated the remote administration of the server conducted from a laptop with a LAN connection, as well as the server behavior after receiving the "alarm" signal. We did not find any unexpected surprises. Upon receiving the "alarm" signal, the server restarted and became available online. The encrypted partition was not accessible until the access keys were remotely loaded from the management console. The system does not offer any other methods for loading the keys, which requires several manual steps each time the server is restarted, which could be seen as an inconvenience. However, this protocol provides an additional layer of security, because it ensures the data is inaccessible, even when the intruder gains physical access to the server.

Decryption of the disk did not cause any complications. It took approximately three hours and 45 minutes, which was less than the time it took to encrypt the data. The difference in time can be explained by using fewer resources on concurrent tasks performed. This time around, we only used the music player and ICQ program, with sporadic use of the text editor.

We conclude that, in our testing environment, Zserver 5.0 is a straightforward, practical application that does not impair performance of the underlying operating system. Nevertheless, when planning the product installation, we recommend first evaluating expected increases in the CPU workload, as the system has shown it is capable of creating considerable overhead. In the case of a file server that is not equipped with large number of high-speed disks and network interfaces, the performance overhead does not appear to be a critical issue. Yet, if the server performs significant amounts of work, such as serving databases or applications, this factor may be important. And, in any event, it will be necessary to ensure that the smart card module is operable. We recommend contacting the developer to resolve any potential issues that you may come across.