Is a Diskless Environment Secure?

M. Satyanarayanan
Information Technology Centre
19 July 84 01:06

Diskless operation, as pioneered by SUN Microsystems and Apollo Computers, has been shown to be a viable mode of operation. The key to the success of these implementations has been the development of highly specialised lightweight protocols. Special low-level software is used to ensure that very short instruction path lengths are encountered in sending and receiving net disk packets. The effectiveness of these lightweight protocols is impressive: on a SUN, for instance, the throughtput achievable through the net disk driver has been observed to be over *five* times that achievable via FTP. This is particularly impressive in view of the fact that the FTP rates on the SUNs are equal to or better than the FTP rates observed elsewhere.

Turning to an orthogonal issue, we have placed considerable emphasis on network security in the ITC system. The fundamental tool in this effort is encryption: both for authentication as well as for concealing transmitted data. Taking the physical security of VICE servers and VIRTUE workstations as givens, we have the necessary mechanisms to make communications between them immune to network attacks.

In a diskless environment, "physical security of VIRTUE" must include the net disk traffic between a workstation and its disk server. Sending disk blocks in the clear does not meet this requirement. Some form of encryption is essential. Can we hope to perform this encryption fast enough?

The available DES chips claim to have a *maximum* throughput to 2 Mbytes/sec. This completely ignores startup times, as well as all the software overheads. Even so, it would take 8 milliseconds to do the encryption and decryption involved in handling a 4K page fault with page replacement. In practise I would expect the overheads to be much higher: say 20 milliseconds. This figure is approximately the time it takes to make a disk access. Each page fault would thus effectively require an extra disk accesses! It is needless to dwell on the effect this would have on user-perceived performance.

Even if the necessary performance were attainable, a great deal of effort would have to be spent in tuning and perfecting the protocol implementations. Merely taking SUN's disk driver (assuming their sources are available to us) and hacking in encryption code is unlikely to be satisfactory. Note that it is currently perceived that the *processor*, not the disk, is the bottleneck in the SUN disk driver. Incorporating encryption is unlikely to improve matters.

There is then the issue of authentication. Are disk servers treated as VICE servers, and do they insist on authentication handshakes before they will serve workstations? On whose behalf will such authentication be done? The owner of the workstation?

The problem is exacerbated by the need to boot workstations off disk servers. How will the initial authentication be done? Will workstation ROMs contain code for authentication handshakes? Where will passwords be stored? Concern has been expressed over the presence of passwords in the clear in core dumps; their presence in ROMs can hardly cause less anxiety. Note that we CANNOT afford to leave out authentication in the boot sequence. Otherwise the system is vulnerable to Trojan horse attacks by malicious workstations masquerading as disk servers. In fact the entire area of network booting is open to Trojan horsemanship.

Security in a diskless environment is clearly a fascinating research topic. It may ultimately be shown that the abovementioned fears are groundless, and that diskless operation is indeed compatible with security. However, such a statement cannot be made about the present SUN disk server environment.

In view of these observations I recommend that we take one of the following positions:

1. *Make it a policy decision that we are not concerned with security.*
   This will avoid raising false hopes, and will enable us to gain efficiency in other areas, since we will no longer have to do encryption anywhere.

2. *Avoid diskless operation in our Fall deployment.*
   If we insist on it as a long term goal, we should launch an effort to understand and build a secure diskless environment.