VAX/VMS includes a User Environment Test Package, which verifies that the major hardware components of the system are complete, properly installed, and ready for use. This package can be executed as part of system installation, or it can be run in stand-alone mode at any time.

One binary version of the operating system is created and distributed for each major release of VAX/VMS. Patches are applied throuhg an automatic, machine-readable, maintenance update procedure. Each patch checks for the proper version number and revision level, and updates these figures as appropriate.

Security and Control

VAX/VMS provides privilege, protection, and quota mechanisms to limit user access to system-controlled structures in physical memory, system-structured files and volumes, and certain devices. Typically, one or a few users (system managers and/or operators) who maintain the system on a day-to-day basis have unlimited access to the system, while the access rights of the remaining users are strictly limited.

User accounts maintained in a user authorization file constitute the basis for privilege and quota assignment. The system manager can modify this file through services provided by the system. Each user account identifies a user by name and password. To login and gain access to the system, the user must supply this name and password, password can never be displayed. (Even users submitting batch jobs from card readers must supply a name and password.) The password is encoded and does not appear on displays; once logged in, the users can change their passwords. In each user's account, the system manager assigns privileges and sets quotas on activities and structures that consume system resources, e.g., physical memory, CPU time, disk space, etc.

Login security includes breakin detection which allows terminals to be disabled when a breakin attempt is detected. The user is also informed at login as to the last time login was done for the account. Secure serving provides a means to prevent user programs from initating the login process to obtain user-names and passwords.

The System Manager also has the ability to limit each user to specific time of day access, such as allowing a user to only have access to the system from 9 AM to 5 PM.

Access control lists exist and allow more flexible protection for files and devices. These lists also allow for the logging of successful and unsuccessful attempts to access files.