A Classified LAVC with Distributed Diskless Workstations (CLAVC/DDW)

C. K. Haaker (2644) and M. L. O'Malley (DEC)

SAND--88-3054C

DE89 007583

INTRODUCTION

It appears to be possible to set up VAX/VMS workstations in a Local Area VAXcluster (LAVC) configuration such that these workstations can be used to process classified information, and yet remain outside of a vault. If approved by the DOE, this configuration will enable staff to take advantage of the multiwindow, graphics, and batch processing capabilities of VMS workstations ("VAXstations") without having to leave their office areas, thus increasing their productivity.

The proposed configuration (Figure 1) has these requirements:

1. All workstations are VAX/VMS systems running the Security Enhanced VMS (SEVMS) operating system and SNLA security patches

2. The system is set up as a Local Area VAXcluster with one boot node and multiple satellite workstations

3. The boot node VAX is protected within a vault or vault-type room and is the only VAX in the cluster with local disks

4. All satellite VAXes located outside the vault are diskless

5. All I/O devices on the LAVC (tapes, floppy disk drives, printers) are within the vault

6. The Ethernet linking the boot node and VAXstations should be via a PBX system, rather than the usual broadcast medium, in order to provide node isolation

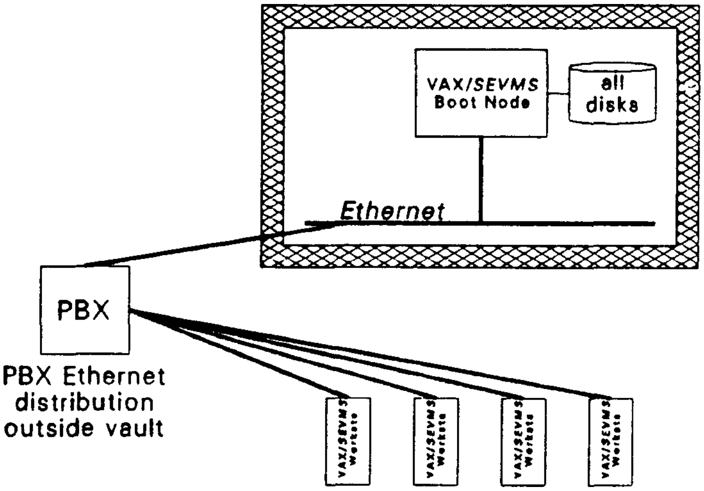
7. Operating restrictions beyond that of a conventional classified VAXcluster are followed, including memory sanitization and restricted availability of non-interactive classified data processing

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

Figure 1

Classified LAVC with Distributed Diskless Workstations



diskless VAX/*SEVMS* workstations

The key to this configuration is that no information, classified or otherwise, is stored on or is removable from systems located outside of a vault. In our opinion, a relatively few weaknesses remain to be addressed; please contact the authors for further information.

LAVC SECURITY FEATURES

A VAXcluster is a tightly coupled group of VAX/VMS processors using shared ("common") system software and linked by a high speed bus (either the CI bus or Ethernet). The need to guarantee synchronous access to shared resources, such as disk volumes and queues, has made cluster integrity and security features an integral part of VMS system software.

A Local Area VAXcluster (LAVC) is a special case of VAXclusters in general (*). The following features distinguish an LAVC from a CI-based VAXcluster:

1. Communications are carried out over an Ethernet instead of a CI
2. One processor (**) serves as the "boot node", which runs the shared system disk and brings up "satellite nodes" by providing a downline load of the operating system software
3. Satellite nodes may be diskless

---

* Under VMS 5.x, "mixed" CI and LAVC clusters are also permissible.

** VMS now permits two boot nodes per LAVC, but the configuration for the CLAVC/DDW assumes only a single boot node, in order to further restrict classified traffic on the Ethernet.

Because multiple LAVCs may exist on a single Ethernet, additional security features not necessary in CI-based VAXclusters have been added to the LAVC software. A unique cluster number and cluster password must be defined for each LAVC. The cluster number can only be obtained from the system by users with SYSPRV privilege; the password is stored in encrypted form in the cluster authorization database. Only privileged users can change either parameter, and must reboot every node in the cluster after the change.

In practice, each LAVC on a given Ethernet should have a unique cluster number; however, if by accident multiple clusters are defined with the same number, their cluster passwords will distinguish them.

Thus, an unprivileged but expert "outsider" (not having inside knowledge of cluster number and password) could not

1. Add another satellite node to an existing cluster. This must be done from a privileged account while logged onto the boot node, and the proper cluster number and cluster password specified.

2. Add another boot node to an existing cluster. This requires knowlege of the LAVC's cluster number and password.

3. Substitute another VAX (with a local system disk containing specially prepared software) for an existing cluster member by shutting down this VAX and booting the substitute in its place. The new node's system disk would need to have the cluster number and password of the LAVC stored in its cluster authorization database.

4. Substituting another VAX with local system disk for an existing cluster member by breaking the connection between a running VAX and the Ethernet and plugging in the new VAX. A VAXcluster is a fragile thing, with a shared

but distributed database of locks. The new system would not have up to date knowledge of these locks, and the rest of the cluster would immediately sense the anomaly and cause the intruder to crash. To reboot into the cluster, the intruder would need to have the proper cluster number and password in its cluster authorization database.

OPERATIONAL RESTRICTIONS

Because the diskless VAXstation satellite nodes will be left unattended outside of the vault, additional protective measures must be implemented. The following is a guide on setting up the Classified LAVC.

MANDATORY RESTRICTIONS

1. Secure VMS operating system
   All systems (boot node and VAXstations) must run the Security Enhanced VMS operating system (SEVMS), and DEC's LAVC software. SEVMS implements mandatory access controls to distinguish the levels and categories of classified information. At Sandia, a few additional patches are added to label magnetic tapes and classify system queues.

2. Physical security for boot node
   The boot node must be inside a vault or vault-type room so that only authorized personnel may gain physical access to it.

3. No local disk storage outside vault
   All cluster satellite nodes outside the vault will be diskless.

4. No I/O devices outside vault
   The satellite workstations will not have local floppy disk drives, magtape or cartridge drives, or printers.

5. No conversational booting of satellite nodes
   The satellite nodes outside the vault will be prohibited from booting conversationally (which could permit an outsider to gain control) by having their SYSGEN parameter PE3 set to zero. This parameter can only be changed by a privileged user.

6. Password protection for cluster
   The cluster number should not be generally known. The cluster password should be protected at the highest level of classified

data stored on the system, and access to it restricted to system management personnel only.

7. Limited number of privileged accounts
   Access to and issuance of privileged accounts will be restricted to system management personnel only. On a VAXcluster, privileges on any node give privileged access on all other nodes, overriding the mandatory access controls. In general, VAXstation users will not need, and should not have, system privileges.

8. Sanitizing memory for unattended systems
   A VAXstation used to process classified, either interactively or via batch job, could have classified information stored in memory which was not overwritten by normal processing. An administrative procedure requiring VAXstation users to, at the end of each working day, run SHUTDOWN, turn off the VAXstation for 60 seconds or more, and then reboot, would clear system memory and permit the VAXstation to run unattended all night. (Similarly, the VAXstation might remain off at night, but be rebooted the following morning, although this is not necessary. An immediate reboot is recommended due to the time it takes for several VAXstations served by a single boot node to receive downline loads of the operating system.)

9. Ethernet security
   Because an ordinary Ethernet is a broadcast medium, a PBX Ethernet is recommended for linking the satellite nodes to the boot node. The PBX, as implemented at Sandia, acts as a security filter so that a particular satellite node receives only information addressed to it.

10. Administrative controls/training
    Users must be adequately informed about these and any other restrictions! They should make sure to reboot workstations every night.

11. Security plan
    All of this should be documented in an approved Security Plan which covers the entire LAVC. An LAVC must be treated as a single unit for security purposes.

OTHER RESTRICTIONS: OPTIONS

The final restriction is to keep classified information off the Ethernet when the office area is unattended. A number of options exist for implementing this goal. Which is used in a particular environment will be a function of the power of the boot node versus the satellite nodes, whether the boot node runs VMS or is just a file server, and the operational needs of the LAVC user community.

There are two sources of classified Ethernet traffic: DECnet communication between a satellite workstation and classified VAXes outside the LAVC, and classified batch processing on a satellite which requires access to disks on the boot node.

PBX Ethernet

The use of a PBX system like that used at Sandia is recommended, as the PBX system isolates individual nodes from the general Ethernet traffic.

DECnet restrictions

DECnet is not actually needed within an LAVC. It can either be shut down entirely on the satellite nodes, or turned off on the satellites during non-working hours.

Batch processing restrictions:

The choice of this option may be based primarily on relative CPU power. Options include

a. All batch queues run on the boot node. No batch processing is allowed on satellites.

b. Classified batch queues run only on the boot node, but satellites may have unclassified batch queues.

c. Any classified batch queues on the satellite nodes are stopped at the end of the workday.

d. No batch processing is allowed.

CONCERNS NOT ADDRESSED

There are some other concerns remaining which are being addressed by groups within Sandia. Those interested should contact the authors.