Securing Your VAXcluster System

VMS
VAXcluster-Related
Security

Introduction

This article discusses security in a VAXcluster system that is part of a larger network of computers. It focuses on the experiences of Digital's Electronic Information Security Group.

In recent months, there has been much publicity dealing with issues relevant to the vulnerabilities of computer systems and the various types of attacks used to gain access to those systems.

Electronic Information Security Group

Digital's Electronic Information Security Group is primarily responsible for securing the corporation's voice and data networks against unauthorized access. The data network comprises over 39,000 computers distributed worldwide.

The group also works with Digital's customers, giving on-site presentations or sending advice through a Sales representative.

The group's scope is international; it works with a similar Digital group located in Europe. Their work sometimes puts them in contact not only with federal, state, or local law enforcement agencies, but also with their counterparts in various foreign countries.

They also cooperate with other computer vendors in the sharing of information. With the growth of *open systems* and the linking of many different kinds of computers from many different vendors, security is becoming an intercompany issue as well.

The Electronic Information Security Group provides recommendations and feedback of its findings to VMS operating system engineers and other Digital personnel as required.

With backgrounds as diverse as police detective, system manager, engineer, network consultant, and educator, the group's investigators mesh talents effectively.

System Invaders

The public's impression of *hackers* who invade systems is based on movie portrayals of fun-loving, innocent teenagers. However, many real-life hackers are highly trained professionals who are hired full-time to do their work, posing real threats to the integrity of systems. They do not always work alone; there are tight networks of hackers where methods and information are freely shared.

The Electronic Information Security Group has identified four categories of invaders, increasingly harmful in the following order: browsers, disgruntled employees, hackers/crackers, and thieves. Fortunately, even though invaders are troublesome, most of them appear to be browsers.

For the most part, browsers enter your network and systems to look around and see if there is anything interesting for them to read or take. They do not usually hurt the systems or information they are accessing and do not want to be found out.

When current or former employees become vindictive over an employment situation, they may delete, alter, or destroy data residing on the system.

Hackers/crackers enter the network and systems to do specific damage, such as alter data in sensitive files or plant trap doors, Trojan horses, worms, or viruses. Their main objective is to leave a hole for them to continue to come back into the system without your knowledge. They also like to use network resources, such as a system's outgoing modem, to defray the cost of long distant calls from their modems while hacking into other locations.

The thieves enter systems for a variety of reasons. One popular reason is to take software products and proprietary information located on the systems. In doing so, they attempt to cover their tracks by damaging the system in some way before they finish their work. This usually causes havoc and destroys any audit trails that may be left behind.

VAXcluster Systems

A major advantage of VAXcluster systems is the high availability of data to potentially many more numbers of users than with single, isolated systems. Also, computer resources that would otherwise be spread over single systems tend to be more centralized in a VAXcluster system. For these reasons, however, the impact can be great if a VAXcluster node is invaded. The whole VAXcluster system can become unavailable to users during investigations of break-ins. Also, the centralized data may make it easier for intruders to find what they are looking for. Therefore, it is important to pay attention to security, as discussed in the Addressing Security Issues section of this article.

When a VAXcluster node is invaded and the invasion is serious, it is customary to shut down all the systems to *reverify* critical applications and to regain control over the system. This guarantees integrity of the data that flows through the network.

If a break-in is suspected, your plan of action for rebuild should include all of the following:

- Shut down DECnet and disconnect all dial-ins and other external connections.
- Reinstall the operating system and all layered products from trusted media.
- Ensure all mandatory security updates for the operating system have been installed.
- Reauthenticate and reenter all system user authorization file (SYSUAF) entries.
- Change all system account and user passwords.
- Acquire system software that is not available from trusted secure media directly from the developer and validate source code.
- Examine all command procedures to ensure integrity.
- Change terminal-server passwords or implement where applicable.
- Ensure that any additional software that installs with privileges is examined by the supplier and that a recompiled version is supplied.

- Eliminate all unnecessary privileged accounts, and remove all proxies to the privileged accounts.
- Ensure all security features for the system are turned on, and bring the system back up on the network.

Addressing Security Issues

Consider the following items to make your VAXcluster system more secure.

- Make security a priority at your site; it is often a side issue for system managers. Five to ten hours per week is not too much time to spend on security-related activities for the average VAXcluster system. Think of the time spent as insurance, and compare it to the expense of having to cope with the consequences of undetected break-ins.

  This time can be spent examining the system authorization file to see, for example, what accounts have been created. (Look especially at privileged accounts.) You can also check the security, error, network-server, and accounting log files for discrepancies and unusual activity. Look at login failures; see if new files have been unaccountably added to a directory. As a VAXcluster system grows larger, it may be necessary to assign more time or people to these activities.

  If you have more than one VAXcluster system, it may be advantageous to prioritize security activity. For example, you may want far greater protection on a system dedicated to research and development than on one specified for general computing.

- Although VAXcluster systems are good for centralizing resources, you might consider spreading resources and people to avoid a big impact on the system in the event of a security breach. Make yourself a harder target by possibly having multiple VAXcluster systems, rather than pooling all resources. For example, it may make sense to have separate VAXcluster systems for research and development, general purposes, and engineering.

- Written policies and procedures are absolutely necessary in doing any type of enforcement. Examples of some important policies to initiate are:

  — Information security policy
  — New accounts procedure
  — Account expiration procedure
  — External connections policy
  — Incident reporting policy
  — Incident escalation procedures
  — Password integrity procedure
  — Disaster/recovery plans

- Passwords

  VAXcluster systems often accommodate more users than a single system does. There is greater likelihood that *somebody* will use a simple password, making it easy for an invader to guess it and enter the system and to go from there to a larger network. Therefore, your site should manage passwords well.

- — Use the *expiration date* password feature.
- — Use special characters, such as hyphen (-), dollar sign ($), and numbers, within passwords or include phrases.
- — Use nondictionary words.
- — Do not use personal information, such as names of pets, sports teams, hobbies, street address, cars, spouse, and so on.
- — Use more than 12 characters.
- — Use the *system password* feature (SET PASSWORD/SYSTEM command).
- — Let the system generate passwords (SET PASSWORD/GENERATE command).
- — Use primary and secondary passwords (SET PASSWORD/SECONDARY command).
- — Use terminal server passwords.

- Welcome Messages

  The *welcome message* that appears on users' terminals at login is possibly a misnomer It might serve better as a warning message, giving notice to potential intruders and excluding sensitive information, such as the system name or location or even the company name. Consider creating the same login message for every system at your site.

- VAX Notes

  Intruders obtain information in a surprising number of ways. It is worth pointing out that a VAX Notes user with obvious authority on a subject can tip readers off to the location of certain kinds of information. A reader can obtain the noter's node name by looking at the top of the VAX Notes reply; therefore, it is a good idea for users to *note* from nonsensitive nodes whenever possible.

- Mail

  Intruders also gain information through mail messages, for example, additional addresses from the message header that can lead to sensitive data. Pay attention to users who complain that someone has been reading their mail or that they have not been receiving messages other users say they have sent.

  Also, intruders have gained access to legitimate accounts and sent mail messages throughout the network to obtain further information. Verify the need for sending information that might include passwords, proprietary data, and so on before sending the information.

- File access and protection schemes should be used to determine the type or extent of access a user has to system resources. The user authorization file (UAF) determines which users can log into the system. It also defines characteristics, such as default disks, directories, user identification code (UIC), and privileges. In conjunction with the UAF, the UIC further determines access and provides the basis of clusterwide file protection. Residing in the system rights database file, the UIC determines the degree of access to resources. Therefore, system managers can use the UAF and UIC to carefully restrict system privileges and access to systemwide resources.

- In addition to UAF and UIC features, the use of access control lists (ACLs) provides the system manager the flexibility to grant or deny access to specific users for specific resources or objects. Protected objects can include files, volumes, disks, tapes, mailboxes, and queues.

- User education is the most important piece in securing your system or VAXcluster system. Users must be able to recognize and react quickly to situations when they occur. They are the first line of defense in protecting your systems. Training programs should be well defined for the users and system managers so that they address the security responsibilities adequately.
- Become a *moving target*. Change networking routes. Change system and user passwords regularly. Find out who is logged into your system during the early hours of the morning. Do not be predictable in doing things; vary your times and do unscheduled routines.

The Future

In the future, there will be more new computer users who are less sophisticated. There will be more sophisticated workstations and personal computers that can access large systems on a network, including VAXcluster systems. The users need to be made aware of security issues and taught to do their part to keep the network secure. As has been said many times, the network is only as strong as the weakest node.

Also in the future, use of encryption will increase to maintain integrity of data between systems and other networks. In addition, authentication solutions will be more widely used and based on physical devices such as smart cards and biometric devices, and on software technology.

Computer technology is making more and more use of open system interfaces, making security a critical issue for the future. New products will have security as a major selling feature.