close window

IBM Systems MAGAZINE

Cover Story

Print

Hardening AIX Security

New features in AIX v6 heighten open-systems security

October | November 2007 | by Jaqui Lynch

The new functions offered in the AIX* v6 beta go a long way toward helping secure systems and I encourage everyone to consider using many of these features, particularly AIX Security Expert, which will perform some of the tasks we manually do today.

In previous articles I've explained the importance of hardening AIX security and implementing additional security mechanisms. I'm a great believer in adding multiple layers of security incorporating firewalls and then layering on additional security mechanisms such as secure shell (SSH), TCP wrappers and removing or disabling many insecure and/or unnecessary functions. In AIX v6 and v6.1 IBM has added many features and functions to improve security and assist in protecting the system against attackers.

Security Before v6

Prior to AIX v6 many security enhancements were made in AIX v5.3, including:

Auditing - The key items here are the AIX audit framework and the new AIX Security Expert. Security Expert, introduced with AIX v5.3 tl05, is a set of policy-based rules that can be implemented on your system simply by setting the level to one of the default options (low, medium, high). Once the levels are set it's possible to build an XML file of the policies to use for future consistency checking. The implementation of medium or high security disables many network-level functions as well as other applications so this should be tested thoroughly first.

AIXpert is a quick and reliable way to harden security of the system and monitor it on an ongoing basis. (AIXpert provides an option of recheck the

security policies of the system against the defined configuration information.) AIX v5.3 also supports Stack Execution Disable feature from 2005, which helps protect against buffer overflow-based attacks and vulnerabilities.

Access control - AIX v5.3 supports discretionary-access control (DAC) and provides for multiple types of access-control lists on file objects. Note that AIX natively supports NFS4 ACL for JFS2 filesystems providing for inheritance and other capabilities.

Encryption and crypto - For awhile the AIX OS and the IBM* System p* platform have supported various crypto cards to provide faster encryption activities. In 2007, the AIX OS released PKCS #11 support for 4764 Crypto card. In AIX v5.3 IBM also introduced the Crypto library in C (CLiC) support with FIPS certification for encryption.

Identification and authentication - This primarily consisted of DAC, which incorporates local passwords, LDAP integration, Kerberos and many of enhancements to the length of passphrases. With AIX v5.3 (introduced in November 2007), it will support greater than eight-character passwords and different password-hashing algorithms. System administrators can configure up to 255-character passwords and choose hashing-algorithms to be one of the SHA1/256/512, MD5, Blowfish, etc.

Integrity checking - This feature's trusted computing base (TCB) assists in creating a database of file attributes, provides periodic verification of the system state against the database and detects Trojan horses and other malicious programs on disk.

Mandatory access control - Also known as multi-level security, this refers to the various certifications such as Labeled Security Protection Profile certification. AIX v5.3 provides label-based security solutions through a non-IBM third-party product, Pitbull Foundation Suite from Argus Systems (ISSI). This combination has been certified for LSPP EAL4+ Profile.

Network security - Network security incorporates IP security, OpenSSH, IP v6, TCP wrappers, IP filters, Secure TCP and AIX Security Expert.

System hardening - AIX v5.3 t106 introduced the File Permissions Manager tool fpm, which lets users configure the system security to high, medium or low settings. It's controlled based on the levels of the number of active setuid programs (e.g., in the high level, fewer than 100 programs have the setuid bits turned on).

What's New in v6?

The new and enhanced areas include:

Auditing - AIXpert has been enhanced to provide more levels, one of which assists with CobiT/Sarbanes-Oxley (SOX) compliance requirements. The upgraded AIXpert also provides better interfaces to plug into customer security configuration information and a framework for ISVs to add software-security configurations.

Access control - Implementing enhanced role-based access control (RBAC) lets administrators define policies to delegate system administration and resource-management activities to non-root users. AIX v6.1 provides for more than 150 fine granular controls to define roles and also supports centralizing RBAC policies on a LDAP server. Enhanced RBAC is required to implement workload partitions (WPARs) and is now the default when the system is installed.

Encryption and crypto - CLiC has been enhanced to include the PCKS11-based cryptographic framework. CLiC is also a prerequisite to implement the new encrypted filesystem.

File encryption - AIX v6.1 supports Encrypted File System (EFS) natively on a JFS2 filesystem, which provides seamless encryption of files and directories using AES and RSA algorithms. This feature depends on the CLiC libraries.

Intentification and authentication - AIX v6.1 supports greater than eight-character passwords and passphrases.

Integrity checking - A new feature called Trusted Execution provides for integrity verification. Customers can choose policies to enable checks at execution time (e.g., a policy to implement checks during all loads of kernel extensions that fails the loads that don't match the hash). Unlike TCB, this feature doesn't require an install option to be selected. AIX ships SHA256 hashes for important system files signed by IBM as part of the AIX OS.

Mandatory access control - AIX v6.1 provides for integrated multilevel security capabilities through the Trusted AIX environment, which provides for label-based mandatory access control (MAC), partitioned directory, labeled printing, trusted networking IPv4 and IPv6), etc.

Network security - Network security is improved by secure FTP, Secure by Default and the enhancements to AIX Security Expert.

System hardening - AIXpert is enhanced to include CobiT-SOX level security along with the capability to better customize the security policies. Also, two

new options have been added - Secure by Default, an install option, and Trusted AIX.

AIX v6 Enhancements

Of the new security features in AIX v6, certain improvements are especially noteworthy:

Trusted Execution - Trusted Execution aims to ensure important binaries aren't altered. The key to this is the Trusted Signature Database (TSD), which includes all of the AIX system files. Other critical files can be registered with the database and regular checks can be run to ensure prompt notification of any alterations. The trustchk - a command adds things to the TSD.

Trusted AIX - This provides a trusted base for AIX that includes the removal of the concept of root, uses mandatory access controls and requires the implementation of auditing. With mandatory access control and mandatory integrity control, access is determined by the data's sensitivity label and the compartment (typically a group or department). Trusted AIX introduces the concept of integrity labels that provide granular definitions for how a user or process can modify an object (i.e., can they read, write, append or remove).

RBAC - Enhanced RBAC allows specific roles to be allocated and replaces and enhances many of the functions provided by tools such as sudo. It's now possible to set and control privileges for processes, files and devices. At login time no role is assigned so the user has no real privileges by default. Instead, the swrole command is used to switch into the correct role or roles so that the user can perform the necessary privileged commands. This feature allows for multiple administrators and provides tiered security levels based on the functions a user needs to perform. Since everyone uses their own account and nobody logs on as root, it's possible to provide a full accounting of who did what and when, which is something required by auditors.

RBAC has three key elements - authorizations, roles and privileges. Authorizations are used to grant access to commands or functions that one needs to perform. Several predefined system authorizations start with AIX at the top level. If you've been using RBAC in earlier AIX releases, the authorizations must be migrated to the new format. Roles are assigned to a user and act as a container for a set of authorizations. Privileges are used to grant the power to a process to perform certain privileged operations. When users issue a swrole they receive the authorizations and privileges assigned to that role and they then have the necessary access. Once they switch out of that role the authorizations and privileges are removed.

While it's possible to have all of the RBAC information stored in an LDAP database, the default files are in /etc/security and are called privfiles, privdevs, authorizations, privcmds and roles. Before privileges can be set up for a file, that file needs to exist so the files must be created ahead of time. It should be noted that privileges are now granted by the kernel so it's important to update the kernel security table using the setkst command once any changes are made. Useful commands to research are: lsrole ALL, lssecattr, swrole, ls - ltra, and swrole. AIX v6.1 also provides for graphical interfaces to configure and manage roles, etc.

Secure by Default (SBD) - SBD is an installation option that ensures the system is only installed with a minimum group of filesets (about 100 of them) to minimize security risks. It's a well-known security approach where you get nothing until you explicitly add it. Since most of the network filesets aren't installed, it will be necessary to install those individually once it's determined which ones are needed.

File Permission Manager - File Permission Manager reduces the programs that have setuid bits set on. The fpm command can be run and set to various levels to ensure that suid bits are removed only where necessary. The bits can be set back to the default settings using the "fpm - l default" command if the results seen aren't what is expected.

EFS - A critical new function long overdue, EFS is a filesystem with a new attribute that indicates when the files in this filesystem are to be encrypted as they contain sensitive data. EFS is only available for JFS2 filesystems and the EFS is created using a new filesystem type of efs. The filesystem is encrypted on a per-file basis and the "ls - aU" command can be used to see whether a file is encrypted. Instead of showing permissions such as rwxr-xr-x the file would show as rwxr-xr-xe.

EFS requires the installation of the CLiC library and the use of keys for encryption. Two new commands have been added - efsmgr and efskeymgr. efsmgr manages the encryption of files, directories and filesystems including enabling EFS and setting up inheritance. efskeymgr manages and administers the keys used for EFS. Keystores can be created for various users, including AIX groups, allowing administrators to share access for the entire group. Provided the users have the necessary keys, use of the EFS should be transparent to them.

Inheritance isn't turned on by default for the EFS. If it's desired, then the "efsmgr - s - E" command should be used once the filesystem is set up to ensure that all files are encrypted. Inheritance can be set on the filesystem or a directory in the filesystem. EFS has to be explicitly enabled using the

"efsenable - a" command.

Chapter 2 of the "AIX v6 Advanced Security" Redbook* publication gives more detail on setting up and using the EFS.

Secure FTP - Secure FTP encrypts both the data and command channels to provide secure file transfer capabilities. Secure FTP is built on OpenSSL technology and provides an alternative to regular FTP access for those who don't want to require users to install SSH. While secure FTP isn't a replacement for SSH it's very useful when you have to communicate with outside systems that don't have SSH capabilities but that offer ftps (ftp with ssl). The ftp - s command uses the OpenSSL libraries. You can enable secure FTP to use TLS as long as you have a certificate authority set up.

Part of the Overall Solution

This is a sampling of the offerings in AIX v6 to enhance security. When these are added to a coherent security plan that layers on additional features (e.g., network security, firewalls, TCP wrappers and SSH), it's possible to reach a high level of security that should help keep attackers away from your systems.

For More Information

For more about open systems security, check out Technical Editor Ken Milberg's two-part feature on security with a RHEL5 server on a System p platform. The first half of the article originally appeared online in September (www. ibmsystemsmag.com/opensystems/administrator/16858p1.aspx).

References

pSeries Information Center (AIXpert)

pSeries Information Center (General Security)

SG24-7430 AIX v6 Advanced Security Draft (Aug0807)

"Stronger Security With OpenSSH"

"Building Reinforcements"

Open Beta for AIX v6.1

website by MSP TechMedia under license from International Business Machines Corporation.