Security Profile Evaluation Assurance

Contributed by Michael Felt

Overview

System administrators can install a system with the Base AIX Security (BAS) and Evaluation Assurance Level 4+ (EAL4+) option or Labeled AIX Security (LAS) and Evaluation Assurance Level 4+ (EAL4+) during a base operating system (BOS) installation. A system with these options has restrictions on the software that is installed during BOS installation, plus network access is restricted.

- Installing additional software on a BAS/EAL4+ compliant system

The administrator can install additional software on the BAS/EAL4+ compliant system. If the software is not run by the root user or with root-user privileges, this will not invalidate the BAS/EAL4+ compliance. Typical examples include office applications that are run only by regular users and have no SUID components.

Additionally, installed software that runs with root-user privileges invalidates the BAS/EAL4+ compliance. This means, for example, drivers for the older JFS should not be installed, as they are running in kernel mode. Any applications granted with one or more privileges through the /etc/security/privcmds is not acceptable. Additional daemons that are run as root (for example, an SNMP daemon) also invalidates the BAS/EAL4+ compliance. A BAS/EAL4+ enabled system cannot be upgraded (normally).

A BAS/EAL4+ compliant system is rarely used in the evaluated configuration, especially in a commercial environment. Typically, additional services are needed, so that the production system is based on an evaluated system, but does not comply with the exact specification of the evaluated system.

-
LAS compliant system