Linux Security Module Usage

The Linux Security Module (LSM) framework provides a mechanism for various security checks to be hooked by new kernel extensions. The name "module" is a bit of a misnomer since these extensions are not actually loadable kernel modules. Instead, they are selectable at build-time via CONFIG_DEFAULT_SECURITY and can be overridden at boot-time via the `"security=..."` kernel command line argument, in the case where multiple LSMs were built into a given kernel.

The primary users of the LSM interface are Mandatory Access Control (MAC) extensions which provide a comprehensive security policy. Examples include SELinux, Smack, Tomoyo, and AppArmor. In addition to the larger MAC extensions, other extensions can be built using the LSM to provide specific changes to system operation when these tweaks are not available in the core functionality of Linux itself.

The Linux capabilities modules will always be included. This may be followed by any number of "minor" modules and at most one "major" module. For more details on capabilities, see `capabilities(7)` in the Linux man-pages project.

A list of the active security modules can be found by reading `/sys/kernel/security/lsm`. This is a comma separated list, and will always include the capability module. The list reflects the order in which checks are made. The capability module will always be first, followed by any "minor" modules (e.g. Yama) and then the one "major" module (e.g. SELinux) if there is one configured.

Process attributes associated with "major" security modules should be accessed and maintained using the special files in `/proc/.../attr`. A security module may maintain a module specific subdirectory there, named after the module. `/proc/.../attr/smack` is provided by the Smack security module and contains all its special files. The files directly in `/proc/.../attr` remain as legacy interfaces for modules that provide subdirectories.

System Message: ERROR/3 (D:\onboarding-resources\sample-onboarding-resources\linux-master\Documentation\admin-guide\LSM\[linux-master][Documentation][admin-guide][LSM]index.rst, line 40)

Unknown directive type "toctree".

```
.. toctree::
   :maxdepth: 1

   apparmor
   LoadPin
   SELinux
   Smack
   tomoyo
   Yama
   SafeSetID
```