USBGuard

Configuration

usbguard-daemon.conf – USBGuard daemon configuration file

The `usbguard-daemon.conf` file is loaded by the USBGuard daemon after it parses its command-line options and is used to configure runtime parameters of the daemon. The default search path is */etc/usbguard/usbguard-daemon.conf*. It may be overridden using the `-c` command-line option, see usbguard-daemon(8) for further details.

Options

- `RuleFile=<path>` The USBGuard daemon will use this file to load the policy rule set from it and to write new rules received via the IPC interface.
- `IPCAllowedUsers=<username> [<username> ...]` A space delimited list of usernames that the daemon will accept IPC connections from.
- `IPCAllowedGroups=<groupname> [<groupname> ...]` A space delimited list of groupnames that the daemon will accept IPC connections from.
- `ImplicitPolicyTarget=<target>` How to treat devices that don't match any tule in the policy. Accepted values: allow, block, reject.
- `PresentDevicePolicy=<policy>` How to treat devices that are already connected when the daemon starts:
  - allow - authorize every present device
  - block - deauthorize every present device
  - reject - remove every present device
  - keep - just sync the internal state and leave it
  - apply-policy - evaluate the ruleset for every present device

- `PresentControllerPolicy=<policy>` How to treat USB controllers that are already connected when the daemon starts:
  - allow - authorize every present device
  - block - deauthorize every present device
  - reject - remove every present device
  - keep - just sync the internal state and leave it
  - apply-policy - evaluate the ruleset for every present device

Security Considerations

The daemon provides the USBGuard public IPC interface. Depending on your distribution defaults, the access to this interface is limited to a certain group or a specific user only. Please set either the *IPCAllowedUsers* or *IPCAllowedGroups* options to limit access to the IPC interface. *Do not leave the ACL unconfigured as that will expose the IPC interface to all local users and will allow them to manipulate the authorization state of USB devices and modify the USBGuard policy*.

Example

The following configuration file will tell the USBGuard daemon to load rules from file */etc/usbguard/rules.conf* and allow only users from the *usbguard* group to use the IPC interface.

```
RuleFile=/etc/usbguard/rules.conf
IPCAllowedGroups=usbguard
```