NAME

apparmor_xattrs − AppArmor profile xattr(7) matching

DESCRIPTION

AppArmor profiles can conditionally match files based on the presence and value of extended attributes in addition to file path. The following profile applies to any file under ‘‘/usr/bin’’ where the ‘‘security.apparmor’’ extended attribute has the value ‘‘trusted’’:

```
profile trusted /usr/bin/* xattrs=(security.apparmor="trusted") {
        # ...
}
```

Note that ‘‘security.apparmor’’ and ‘‘trusted’’ are arbitrary, and profiles can match based on the value of any attribute.

The xattrs value may also contain a path regex:

```
profile trusted /usr/bin/* xattrs=(user.trust="tier/*") {

        # ...
}
```

The **getfattr** (1) and **setfattr** (1) tools can be used to view and manage xattr values:

```
$ setfattr −n 'security.apparmor' −v 'trusted' /usr/bin/example−tool
$ getfattr −−absolute−names −d −m − /usr/bin/example−tool
# file: usr/bin/example−tool
security.apparmor="trusted"
```

The priority of each profile is determined by the length of the path, then the number of xattrs specified. A more specific path is preferred over xattr matches:

```
# Highest priority, longest path.
profile example1 /usr/bin/example−tool {
        # ...
}

# Lower priority than the longer path, but higher priority than a rule
# with fewer xattr matches.
profile example2 /usr/** xattrs=(
        security.apparmor="trusted"
        user.domain="**"
) {
        # ...
}

# Lowest priority. Same path length as the second profile, but has
# fewer xattr matches.
profile example2 /usr/** {
        # ...
}
```

xattr matching requires the following kernel feature:

```
/sys/kernel/security/apparmor/features/domain/attach_conditions/xattr
```

KNOWN ISSUES

AppArmor profiles currently can’t reliably match extended attributes with binary values such as security.evm and security.ima. In the future AppArmor may gain the ability to match based on the presence of certain attributes while ignoring their values.

SEE ALSO

apparmor (8), **apparmor_parser** (8), **apparmor.d** (5), **xattr** (7), **aa−autodep** (1), **clean** (1), **auditd** (8), **getfattr** (1), **setfattr** (1), and <https://wiki.apparmor.net>.