Sudo Privilege Policy

This is a draft document

Background

Sudo is a program used to grant root privileges on unix-based systems. Access can be granted to run an individual command, groups of commands, or arbitrary commands. This policy attempts to strike a balance between functionality and security while recognizing the need to protect all users of the SoIC systems against incorrect or malicious use of sudo privileges. Furthermore, sudo provides logging that provides valuable auditing records that can be useful in the event of resulting system problems and as a record of system changes. For this reason, the use of sudo to get root shells is discouraged because any information about what was done to the system is lost.

Definitions

Security Levels

The risk associated with granting access to a particular set of commands is defined as follows:

1. **Very High** - The user has full access to the local system and can become other users with no ability to monitor activities. Furthermore, access to both local and network data for other users is possible.
2. **High** - The user has the ability to gain full access to the local system and become other users but privilege escalation would be detectable via system logs.
3. **Medium** - The user does not have full access to the local system and can only become other users as specified (ie. for group/project accounts). Note that malicious use of commands in this category could result in unauthorized privilege escalation but such activity would require deliberate circumvention of privilege restrictions and would be detectable via system logs.
4. **Low** - The user has limited access to the local system and cannot become other users. The user does have the ability to modify and disrupt services on the local system.

System Configurations

Allowable access levels are dependent on the system configurations which are defined in the following document:

**Supported Linux Configurations**

The following configurations are referenced in this sudo policy document:

1. **Unified Server**
2. **Unified Workstation**
3. **Hybrid**
4. **Standalone**

Systems in the **Self-Managed** category are not managed by SoIC staff so are not subject to this policy.

Sudo Command Groups

Sudo allows the definition of command groups and access can be granted to the specified collection of commands. The following table defines standard command groups, their function, and the associated security level.

<table>
<thead>
<tr>
<th>Name</th>
<th>Function</th>
<th>Commands</th>
<th>Security Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>UNRESTRICTED</td>
<td>Full access</td>
<td>All</td>
<td>Very High</td>
</tr>
<tr>
<td>FULL</td>
<td>Access to all commands but no shells</td>
<td>All except shells</td>
<td>High</td>
</tr>
<tr>
<td>FILESYSTEM</td>
<td>Manage files and directories</td>
<td>chmod, chown, chgrp, cp, rm, cat, ls, rm, rmdir, mkdir, setfacl, getfacl</td>
<td>Medium</td>
</tr>
<tr>
<td>SU</td>
<td>Log in as another user (group or project account)</td>
<td>su (limited to specific group or project username)</td>
<td>Medium</td>
</tr>
<tr>
<td>HTTPD</td>
<td>Manage web server</td>
<td>service, apachectl, sudoedit /etc/httpd/*</td>
<td>Low</td>
</tr>
<tr>
<td>MYSQL</td>
<td>Manage mysql database</td>
<td>service, mysql, mysqladmin, sudoedit /etc/my.cnf</td>
<td>Low</td>
</tr>
</tbody>
</table>
### Access Matrix

The level of access permitted is a function of various factors, including the status of the user (faculty, staff, RA, graduate students, undergraduate students), the owner of the system, the sponsorship of the user, and the configuration of the machine. The following table lists the maximum security level allowed as a function of the system configuration and user classification:

<table>
<thead>
<tr>
<th>User Classification</th>
<th>Unified Server</th>
<th>Unified Workstation</th>
<th>Hybrid</th>
<th>Standalone</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT Staff</td>
<td>Very High</td>
<td>Very High</td>
<td>Very High</td>
<td>Very High</td>
</tr>
<tr>
<td>Faculty/Non-IT Staff/RA</td>
<td>Medium</td>
<td>High</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Graduate Students</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
<td>High</td>
</tr>
<tr>
<td>Undergraduate Students</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
</tr>
</tbody>
</table>

Notes:
- All sudo access requires approval by the system owner or, in the case of SoIC-purchased systems, approval of the Director of IT.
- All student sudo access requires sponsorship by a member of the faculty or approval by the Director of IT.
- Exceptions will only be granted in extenuating circumstances with faculty sponsorship and with approval of the Director of IT.

### IU Data Privacy Policies

Indiana University has Information and IT Policies in place regulating the security of data on all IU systems. The two policies most related to the granting of sudo permissions are:

- **IT-02 – Misuse and Abuse of IT Resources**
- **IT-07 – Privacy of Electronic Information and Information Technology Resources**

All users of IU computing systems, including those granted sudo permissions, are required to operate within these policies. Anyone receiving sudo permissions with a security level of *medium* or higher will be asked to acknowledge that they understand these policies and agree to be bound by them.