SUSE

Understanding SELinux Basics

WHAT?

This article provides basic information about Security-Enhanced Linux.

WHY?

You want to understand SELinux and how to configure it on SUSE Linux Micro.

EFFORT

It takes approximately 40 minutes to read this article.

Publication Date: 26 Nov 2024

Contents

1 About SELinux

SELinux was developed as an additional Linux security solution that uses the security framework in the Linux kernel. The purpose was to allow for a more granular security policy that goes beyond the standard Discretionary Access Controls (DAC), the traditional file permissions of owner/group/world, and read/write/execute.

SELinux uses labels attached to objects (for example, files and network sockets) to make access control decisions.

The default action of SELinux is to deny any access. SELinux allows only actions that were specifically allowed in the SELinux policy. Another feature of SELinux that increases security is that SELinux allows strict confinement of processes up to the point where the processes cannot access files of other processes on the same system.

SELinux was designed to enhance existing security solutions, not to replace them. For example, discretionary access control (DAC) is still applied, even if the system is using SELinux. If DAC denies access first, SELinux is then not used as the access was already blocked by another mechanism.

2 Getting SELinux

SELinux is installed by default when installing SUSE Linux Micro by YaST or is part of the pre-built images.

If SELinux is not set up on your system, run the following command:

```
# transactional-update setup-selinux
```

Reboot your system after the command has finished. The command installs the SELinux policy if it is not installed, sets the `enforcing` SELinux mode and rebuilds `initrd`.

3 SELinux modes

SELinux can run in one of three modes: `disabled`, `permissive` or `enforcing`.

Using the `disabled` mode means that no rules from the SELinux policy are applied and your system is not protected. Therefore, we do not recommend using the `disabled` mode.

In the `permissive` mode, SELinux is active, the security policy is loaded, the file system is labeled and access denial entries are logged. However, the policy is not enforced and thus no access is actually denied.

In the `enforced` mode, the security policy is applied. Each access that is not explicitly allowed by the policy is denied.

For information about switching between SELinux modes, refer to *Section 3.1, "Changing the SELinux mode"*.

3.1 Changing the SELinux mode

You can switch the SELinux mode temporarily or permanently.

3.1.1 Changing the SELinux mode temporarily

To set SELinux to the `permissive` or `enforcing` mode temporarily, use the command **`setenforce`**.

The **`setenforce`** command has the following syntax:

```
# setenforce MODE_ID
```

where *`MODE_ID`* is *`0`* for the `permissive` mode or *`1`* for the `enforced` mode.

Remember that you cannot disable SELinux using the **`setenforce`** command.

3.1.2 Changing the SELinux mode permanently

To perform changes to the SELinux mode that persists rebooting of the system, edit the `/etc/selinux/config` configuration file. In this file, you can also disable SELinux on your system. However, this action is not recommended. If SELinux is possibly causing issues to your system, switch to the `permissive` mode instead and debug your system.

In the file `/etc/selinux/config`, change the value of `SELINUX` to `disabled`, or `permissive`, or `enforced` as follows:

```
SELINUX=disabled
```

The changes in the file are applied after the next reboot.

Note: Relabeling your system after switching from the `disabled` mode

If you disable SELinux on your system and then enable it later, make sure that you relabel your system. When SELinux is disabled and you perform changes to your file system, the changes are not reflected in the context anymore (for example, new files do not have any context). Therefore, you need to relabel your system by using the **`restorecon`** command, using the `autorelabel` boot parameter, or by creating a file that will trigger relabeling on the next boot. To create the file, run the following command:

```
# touch /etc/selinux/.autorelabel
```

After reboot, the file `/etc/selinux/.autorelabel` is replaced with another flag file, `/etc/selinux/.relabelled`, to prevent relabeling on subsequent reboots.

3.1.3 Verifying the active SELinux mode

To verify the mode, run the following command:

```
# getenforce
```

The command should return `permissive` or `enforced`, depending on the provided *`MODE_ID`*.

3.2 Verifying that SELinux is functional

If you are performing configuration changes, it may be useful to switch to permissive mode. During this time, users might label files incorrectly, and thus cause problems when switching back to enforcing mode.

To return the system back to its secured state, perform the following steps:

1. Reset the security context:

```
>
sudo
restorecon -R /
```

2. Switch to enforcing mode by setting `SELINUX=enforcing` in the `/etc/selinux/config`.
3. Reboot the system and log in again.

4. Run the `sestatus -v` command. It should give you an output similar to the following one:

```
> sudosestatus -v
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             targeted
Current mode:                   enforcing
Mode from config file:          enforcing
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Memory protection checking:     requested(insecure)
Max kernel policy version:      33

Process contexts:
Current context:                unconfined_u:unconfined_r:unconfined_t:s0-
s0:c0.c1023
Init context:                   system_u:system_r:init_t:s0
/usr/sbin/sshd                  system_u:system_r:sshd_t:s0-s0:c0.c1023

File contexts:
Controlling terminal:           unconfined_u:object_r:user_tty_device_t:s0
/etc/passwd                     system_u:object_r:passwd_file_t:s0
/etc/shadow                     system_u:object_r:shadow_t:s0
/bin/bash                       system_u:object_r:shell_exec_t:s0 \
                                -> system_u:object_r:shell_exec_t:s0
/bin/login                      system_u:object_r:login_exec_t:s0
/bin/sh                         system_u:object_r:bin_t:s0 \
                                -> system_u:object_r:shell_exec_t:s0
/sbin/agetty                    system_u:object_r:bin_t:s0 \
                                -> system_u:object_r:getty_exec_t:s0
/sbin/init                      system_u:object_r:bin_t:s0 -> \
                                system_u:object_r:init_exec_t:s0
/usr/sbin/sshd                  system_u:object_r:sshd_exec_t:s0
```

5. If the system is not working properly, check the log files in `/var/log/audit/audit.log`. For more details, refer to SELinux troubleshooting (https://documentation.suse.com/sle-micro/6.0/html/Micro-setroubleshoot/setroubleshoot.html).

4 SELinux security context

The security context is a set of information assigned to a file or a process. It consists of SELinux user, role, type, level and category. This information is used to make access control decisions.

SELinux user

An identity defined in the policy that is authorized for a specific set of roles and for a specific *level* range. Each Linux user is mapped to only one SELinux user. However, one SELinux user can have several roles.

SELinux does not use the list of user accounts maintained by Linux in `/etc/passwd`, but uses its own database and mapping. By convention, the identity name is suffixed with `_u`, for example, `user_u`.

When a new Linux account is created and the SELinux user is not assigned to the account, the default SELinux user is used. Usually, the default value is `unconfined_u`. For a procedure on how to change the default value, refer to *Section 7.5.2, "The* **`semanage login`** *command"*.

role

Defines a set of permissions that a user can be granted. A role defines which *types* a user assigned to this role can access. By convention, the role name is suffixed with `_r`, for example, `system_r`.

type

The type conveys information on how particular files and processes can interact. A process consists of files with a concrete SELinux type, and it cannot access files outside of this type. By convention, the type name is suffixed with `_t`, for example, `var_t`.

level

An optional attribute that specifies the range of levels of clearance in the multilevel security.

category

An optional attribute that allows you to add categories to processes, files and users. A user can then access files that have the same category.

Here is an example of an SELinux context:

```
allow user_t bin_t:file {read execute gettattr};
```

This example rule states that the user who has the context type `user_t` (this user is called the source object) is allowed to access objects of the class *file* with the context type `bin_t` (the target), using the permissions `read`, `execute` and `getattr`.

5 SELinux policy overview

The policy is the key component in SELinux. Your SELinux policy defines rules that specify which objects can access which files, directories, ports and processes on a system. To do this, a security context is defined for all of these.

An SELinux policy contains a huge number of rules. To make it more manageable, policies are often split into modules. This allows the administrator to switch protection on or off for different parts of the system.

When compiling the policy for your system, you will have a choice to either work with a modular policy, or a monolithic policy, where one huge policy is used to protect everything on your system. We strongly recommend using a modular policy and not a monolithic policy. Modular policies are much easier to manage.

SUSE Linux Micro is shipped with the `targeted` SELinux policy.

5.1 Working with SELinux modules

As an administrator, you can switch modules on or off. This can be useful if you want to disable only a part of the SELinux policy and you do not want to run a specific service without SELinux protection.

To view all SELinux policy modules in use, run the command:

```
semodule -l
```

After you get the name of the module you want to switch off, run the command:

```
>
sudo
semodule -d MODULENAME
```

To switch on the policy module, run the command:

```
>
sudo
semodule -e MODULENAME
```

5.2 Creating policies for containers

SUSE Linux Micro is delivered with a policy that, by default, does not allow containers to access files outside the container data. On the other hand, all network access is allowed. Typically, containers are created with bind mounts and should be able to access other directories, like `/home` or `/var`. You may want a possibility to allow access to these directories or, on the contrary, restrict some ports to the container even if SELinux is used on your system. In this case, you need to create new policy rules that enable or disable the access. SUSE Linux Micro provides the Udica tool for this purpose.

The following procedure describes how to create a custom policy for your containers:

1. Make sure that SELinux is in the enforcing mode. For details, refer to *Section 3.1, "Changing the SELinux mode"*.

2. Start a container using the following parameters:

   ```
   # podman run -v /home:/home:rw -v /var/:/var/:rw -p 21:21 -it sle15 bash
   ```

   The container runs with the default policy that does not allow access to the mount points but does not restrict other ports.

3. You can exit the container.

4. Obtain the container ID:

   ```
   # podman ps -a

   CONTAINER ID  IMAGE
               COMMAND     CREATED        STATUS            PORTS               NAMES
   e59f9d0f86f2  registry.opensuse.org/devel/bci/tumbleweed/containerfile/opensuse/
   bci/ruby:latest  /bin/bash   8 minutes ago  Up 8 seconds ago  0.0.0.0:21->21/tcp
    zen_ramanujan
   ```

5. Create a JSON file that Udica will use to create a custom policy for the container:

   ```
   # podman inspect e59f9d0f86f2 > OUTPUT_JSON_FILE
   ```

   For example, substitute *`OUTPUT_JSON_FILE`* with `container.json`.

6. Run Udica to generate a policy according to the container parameters:

   ```
   # udica -j OUTPUT_JSON_FILECUSTOM_CONTAINER_POLICY
   ```

For example:

```
# udica -j container.json custom_policy
```

7. According to the provided instructions, load the policy modules by running:

```
# semodule -i custom_policy.cil /usr/share/udica/templates/
{base_container.cil,net_container.cil,home_container.cil}
```

8. Run a container with the new policy module by using the `--security-opt` option as follows:

```
# podman run --security-opt label=type:custom_policy.process -v /home:/home:rw -v /
var/:/var/:rw -p 21:21 -it sle15 bash
```

6 SELinux Booleans

SELinux Booleans support a flexible policy management approach. For example, Booleans enable you to disable a particular policy on one server, while keeping the same policy active on another one. In other words, a Boolean can be understood as a switch for a policy rule. Instead of changing a particular policy, you can switch it off. In the policy code, Booleans are called a *tunable*. Because Booleans are included in the policy, they are available as soon as a policy is loaded.

The changes to the Booleans value may be persistent or temporary, lasting until the end of the session.

SELinux offers tools that enable you to list and view details or change the state of Booleans. See the following sections for details.

6.1 Working with Booleans

6.1.1 Listing Booleans

You can use the **`getsebool`** or **`semanage`** command to list currently defined Booleans. To list all currently defined Booleans, along with their state, run the following command:

```
# getsebool -a
```

```
abrt_anon_write --> off
abrt_handle_event --> off
abrt_upload_watch_anon_write --> on
...
```

To get more details about particular Booleans, you can use the **`semanage`** command as follows:

```
# semanage boolean -l

SELinux boolean                State   Default     Description

abrt_anon_write                (off  ,  off)       Allow abrt to anon write
abrt_handle_event              (off  ,  off)       Allow abrt to handle event
abrt_upload_watch_anon_write   (on   ,   on)       Allow abrt to upload watch anon write
```

To get the status of an individual Boolean, you can use the following command:

```
# getsebool BOOLEAN_NAME
```

Alternatively, you can just use the **`grep`** command on the **`semanage boolean`** output:

```
# semanage boolean -l | grep BOOLEAN_NAME
```

6.1.2 Toggling Booleans

The commands **`setsebool`** and **`semanage`** can be used to toggle the value of Booleans. You can change the Boolean status persistently or just temporarily until the session ends. To change a Boolean value temporarily, run the following command:

```
# setsebool BOOLEAN_NAMEBOOLEAN_VALUE
```

where *`BOOLEAN_VALUE`* is either `on` or `off`.

To change a Boolean value persistently, run one of the following two commands:

```
# setsebool -P BOOLEAN_NAMEBOOLEAN_VALUE
```

Alternatively, using the **`semanage`** command:

```
# semanage boolean -m --BOOLEAN_VALUEBOOLEAN_NAME
```

where *`BOOLEAN_VALUE`* is either `on` or `off`.

A single Boolean can enable or disable several policy rules. To see which policy rules are enabled or disabled by specific Booleans, use the **`sedispol`** tool to analyze the policy file:

```
# sedispol /etc/selinux/targeted/policy/policy.32
```

As the policy rules are usually huge, we recommend setting an output file by selecting the `f` and specifying a file name. After specifying the file name, press `6`. Then you can inspect the file.

7 Tools for managing SELinux

SUSE Linux Micro provides you with tools to manage SELinux on your system. If the below described tools are not installed on your system, install the tools by running:

```
# transactional-update pkg install policycoreutils-python-utils
```

After successful installation, reboot the system.

7.1 Using the Z option

Where SELinux is installed and configured, you can use the `-Z` to regular commands like **`ls`**, **`id`** or **`ps`**. Using this option, you can display the security context of files or processes. For example, with the **`ls`** command:

```
> ls -Z /etc/shadow

        system_u:object_r:shadow_t:s0 /etc/shadow
```

7.2 The **`chcon`** command

The command name **`chcon`** stands for change context. The command can change the full security context of a file to the value provided on the CLI, or it can change parts of the context. Alternatively, you can provide a file that serves as a reference.

To change the full security context of a file, the command syntax looks as follows:

```
# chcon SECURITY_CONTEXTFILENAME
```

where:

- *`SECURITY_CONTEXT`* is in the format: *`SELinux_USER`*:*`ROLE`*:*`TYPE`*:*`LEVEL`*:*`CATEGORY`*. For example, the context could be: *system_u:object_r:httpd_config_t:s0*.
- *`FILENAME`* is a path to the file whose context should be changed.

To set a security context according to a provided file that serves as a reference, run **chcon** as follows:

```
# chcon --reference=REFERENCE_FILEFILENAME
```

where:

- *REFERENCE_FILE* is a path to a file that should be used as a reference.
- *FILENAME* is a path to the file whose context should be changed.

Alternatively, you can change only one part of the security context. The general syntax of the **chcon** command is as follows:

```
# chcon CONTEXT_OPTIONCONTEXT_PARTFILENAME
```

The options and arguments have the following meaning:

- depending on the context part, *CONTEXT_OPTION* can be any of the following:

  -u resp **--user**
  : denotes that an SELinux user context will be changed on the provided file:

    ```
    # chcon -u system_u logind.conf
    ```

  -r resp **--role**
  : only the role part will be changed in the context of the provided file:

    ```
    # chcon -r object_r logind.conf
    ```

  -t resp **--type**
  : only the type part will be changed in the context of the provided file:

    ```
    # chcon -t etc_t logind.conf
    ```

  -l resp **--range**
  : only the range part of the security context will be changed:

    ```
    # chcon -l s0 logind.conf
    ```

- *CONTEXT_PART* is the particular value of the security context to be set.
- *FILENAME* is a path to the file whose context will be changed.

Note: Using **chcon** on symbolic links

By default, when you change the security context on a symbolic link, the context of the link target is changed and the symbolic link context is **not** changed. To force `chcon` to change the context of the symbolic link and not the link target, use the `--no-dereference` option as shown below:

```
# chcon --no-dereference -u system_u -t etc_t network.conf
```

You can change the context of all files in a directory by using the recursive option:

```
# chcon --recursive  system_u:object_r:httpd_config_t:s0 conf.d
```

7.3 `getenforce` and `setenforce` commands

The `getenforce` command returns the current SELinux mode: `Enforcing`, `Permissive` or `Disabled`.

```
# getenforce

Permissive
```

The `setenforce` command temporarily changes the SELinux mode to enforcing or permissive. You cannot use this command to disable SELinux. Remember that the change persists only until the next reboot. To change the state permanently, follow the description in *Section 3.1, "Changing the SELinux mode"*.

```
# setenforce MODE_ID
```

where *`MODE_ID`* is *`0`* for the `permissive` mode or *`1`* for the `enforced` mode.

7.4 The `fixfiles` script

The script enables you to perform the following tasks with the security context:

- check if the context is correct
- change any incorrect file context labels
- relabel your system if you added a new policy

The script syntax is as follows:

```
# fixfiles [OPTIONS] ARGUMENT
```

where:

- *`OPTIONS`* can be the following:

  `-l` *`LOGFILE`*
  : saves the output to the provided file

  `-o` *`OUTPUT_FILE`*
  : saves to the provided output file the names of all files whose file context differs from the default

  `-F`
  : forces a reset of context

- *`ARGUMENT`* can be one of the following:

  `check`
  : shows previous and current file context for an incorrect label without performing any changes

  `relabel`
  : relabels incorrect file contexts according to the currently loaded policy

  `restore`
  : restores incorrect file contexts to the default values

  `verify`
  : lists all files with incorrect file context labels without performing any changes

7.5 The **`semanage`** command

The **`semanage`** command can be used to configure parts of the policy without the need to re-compile the policy from sources. The command enables you to perform the following tasks:

- manage Booleans by using the `boolean` argument. For details about Booleans, refer to *Section 6.1, "Working with Booleans"*.
- adjust the context of files by using the `fcontext` argument

- manage user mappings using the `login` argument
- manage SELinux users using the `user` argument
- manage SELinux policy modules using the `module` argument

The general command syntax looks as follows:

```
# semanage ARGUMENTOPTIONS [OBJECT_NAME]
```

where:

- *`ARGUMENT`* is one of the following: **`login`**, **`user`**, **`fcontext`**, **`boolean`**, **`module`**.
- *`OPTIONS`* depends on the provided *`ARGUMENT`*. Common options are described in *Common options*.
- *`OBJECT_NAME`*, depending on the provided *`ARGUMENT`*, can be a login name, module name, file name or SELinux user.

COMMON OPTIONS

`-a`, `--add`
: adds a provided object

`-h`, `--help`
: prints the command help

--extract
: displays commands that were used to change the system (Booleans, file context, and so on)

`-l`, `--list`
: lists all objects

`-m`, `--modify`
: modifies the provided object

`-n`, `--noheading`
: modifies the output of the listing operation by omitting headings

`-s`, `--seuser`
: specifies the SELinux user

Other options are specific to particular **`semanage`** commands and are described in corresponding sections.

7.5.1 The `semanage fcontext` command

Using the `semanage fcontext` command, you can perform the following tasks:

- query file context definitions
- add contexts on files
- add your own rules

Changes performed to the file context using the `semanage fcontext` command do not require modifications or recompilation of the policy.

On top of the common options described in *Common options*, the `semanage fcontext` command takes the following options:

`-e`, `--equal`
: The option enables you to use the context of the provided path context to label files in a different directory (the provided target path). For example, you want to assign the same context as `/home` has to an alternative home directory `/export/home`. If you use this option, you need to provide the source path and the target path:

```
# semanage fcontext -a -e /home /export/home
```

`-f`, `--ftype`
: To specify a file type. Use one of the following values:

  - `a` - all files, which is also the default value
  - `b` - a block device
  - `c` - a character device
  - `d` - a directory
  - `f` - regular files
  - `l` - a symbolic link
  - `p` - a named pipe
  - `s` - a socket

7.5.2 The `semanage login` command

The `semanage login` enables you the perform the following tasks:

- Mapping of Linux users on a particular SELinux user. For example, to map the Linux user *tux* on `sysadm_u`, run the command:

```
#
semanage login -a -s sysadm_u tux
```

- Mapping of a group of Linux users on a particular SELinux user. For example, to map users of the *writers* group on `user_u`, run the command:

```
#
semanage login -a -s user_u %writers
```

  The group is then listed in the output of `semanage login -l`, prefixed with the % character.
  Keep in mind that the user group should be primary because mapping SELinux users on supplementary groups may result in incompatible mappings.

```
#
semanage login -m -s staff_u %writers
```

- Mapping of Linux users on a particular SELinux MLS/MCS security range.
- Modifying of the already created mapping. For this purpose, just replace the `-a` option with `-m` in the previous commands.
- Setting the default SELinux user for new Linux users. The usual default SELinux user is `unconfined_u`. To change the value to `staff_u`, run the command:

```
#
semanage login -m -s staff_u __default__
```

7.5.3 The `semanage boolean` command

The `semanage boolean` command is used to control Booleans in the SELinux policy.

The command synopsis looks as follows:

```
semanage boolean [-h] [-n]  [ --extract |
       --deleteall | --list [-C] | --modify ( --on | --off | -1 | -0 ) boolean ]
```

On top of the common options, you can use the following ones specific to the **`semanage boolean`** command:

--list -C
: To display a list of local modifications to Booleans.

-m --on | -1
: To switch the provided Boolean on.

-m --off | -0
: To switch the provided Boolean off.

-D, --deleteall
: To delete all local modifications to Booleans.

The most common usage of the command is to switch on or off a particular Boolean. For example, to switch on the `authlogin_yubikey` Boolean, run:

```
#
semanage boolean -m on authlogin_yubikey
```

7.5.4 The `semanage user` command

The **`semanage user`** command controls the mapping between the SELinux user and the roles and MLS/MCS levels.

On top of the common options described in *Common options*, the **`semanage use`** command takes the following options:

-R [ROLES], --roles [ROLES]
: A list of SELinux roles. You can enclose multiple roles within double quotes and separate them by spaces, or you can use the `-R` several times.

Using this command, you can perform the following tasks:

- Listing the mapping of SELinux users on roles by running:

  ```
  #
  semanage user -l
  ```

- Changing the roles assigned to the `user_u` SELinux user:

  ```
  #
  ```

```
semanage user -m -R "system_r unconfined_r user_r"
```

- Assigning to `admin_u` the role `staff_r` and a category `s0`:

```
#
semanage user -a -R "staff_r -r s0 admin_u
```

- Creating a new SELinux user, for example, `admin_u` with the `staff_r` role. You also need to define the labeling prefix for this user by using the `-P`:

```
#
semanage user -a -R "staff_r" -P admin admin_u
```

7.5.5 The `semanage module` command

The **`semanage module`** command can install, remove, disable or enable SELinux policy modules.

On top of the common options described in *Common options*, the **`semanage fcontext`** command takes the following options:

`-d`, `--disable`
: To disable the provided SELinux policy module:

```
#
semanage module --disable MODULE_NAME
```

`-e`, `--enable`
: To enable the provided SELinux policy module:

```
#
semanage module --enable MODULE_NAME
```

7.6 The `sestatus` command

The **`sestatus`** gets the status of a system where SELinux is running.

The generic syntax of the command looks as follows:

```
sestatus [OPTION]
```

When run without any options and arguments, the command outputs the following information:

```
# sestatus
```

```
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             targeted
Current mode:                   enforcing
Mode from config file:          enforcing
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Memory protection checking:     requested (insecure)
Max kernel policy version:      33
```

The command can take the following options:

-b

Displays the status of Booleans on the system.

-v

Displays the security context of files and processes listed in the `/etc/sestatus.conf` file.

8 Legal Notice

A GNU Free Documentation License

0. PREAMBLE

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or non-commercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "Cover Texts" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A "Transparent" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

A section "Entitled XYZ" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "Acknowledgements", "Dedications", "Endorsements", or "History".) To "Preserve the Title" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or non-commercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent

copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.

B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.

C. State on the Title page the name of the publisher of the Modified Version, as the publisher.

D. Preserve all the copyright notices of the Document.

E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.

F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.

G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.

H. Include an unaltered copy of this License.

I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.

J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.

K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.

L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.

M. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.

N. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.

O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties--for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through

arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements".

6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See https://www.gnu.org/copyleft/.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.

ADDENDUM: How to use this License for your documents

```
Copyright (c) YEAR YOUR NAME.
Permission is granted to copy, distribute and/or modify this document
under the terms of the GNU Free Documentation License, Version 1.2
or any later version published by the Free Software Foundation;
with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts.
A copy of the license is included in the section entitled “GNU
Free Documentation License”.
```

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the “with...Texts.” line with this:

```
with the Invariant Sections being LIST THEIR TITLES, with the
Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.
```

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.