SUSE

SUSE Linux Enterprise Server 15 SP6

AMD Secure Encrypted Virtualization (AMD-SEV) Guide

AMD's Secure Encrypted Virtualization (SEV) allows the memory of virtual machines to be encrypted. SEV with Encrypted State (SEV-ES) goes one step further by encrypting the virtual machine's CPU register content. These technologies increase system security and are ideal for multi-tenant environments such as cloud computing. They enable protection from a variety of cross-VM and hypervisor-based attacks. As an example, a hostile VM that has escaped its hypervisor-enforced confines and is able to read arbitrary memory is unable to steal sensitive data from an SEV or SEV-ES VM.

This document aims to provide a basic understanding of how SEV and SEV-ES work, and how to enable and configure these features. It also mentions certain limitations and restrictions that the use of SEV and SEV-ES causes as compared to non-encrypted virtualization.

Publication Date: December 05, 2024

Contents

1 Introducing SEV

Encryption of computer data stored on disk is a widely deployed feature. However, data in RAM is stored in the clear. This can leave that data vulnerable to software or hardware probing by intruders on the host system, particularly in cloud computing environments where the physical resources are shared by many tenants. Consider a virtual machine of a hostile tenant escaping its sandbox because of a hypervisor bug and searching memory for sensitive data.

AMD's SEV (Secure Encrypted Virtualization) is a technology to protect Linux KVM virtual machines by transparently encrypting the memory of each VM with a unique key. SEV can also calculate a signature of the memory contents, which can be sent to the VM's owner as an attestation that the memory was encrypted correctly by the firmware. SEV is especially relevant to cloud computing environments, where VMs are hosted on remote servers which are not under the control of the VMs' owners. SEV can reduce the amount of trust VMs need to place in the hypervisor and administrator of their host system.

When a virtual machine is processing sensitive data, it can be present in CPU registers as well as memory. If the processing is halted, for example, to service an interrupt or share time with other processes, the virtual machine's CPU register contents are saved to hypervisor memory. This memory is readable by the hypervisor even if SEV is enabled. SEV-ES protects against this scenario by encrypting all CPU register contents when the processing of a virtual machine is halted. SEV-ES builds upon SEV to provide an even smaller attack surface for virtual machines running in a multi-tenant environment.

2 VM host requirements

The VM host hardware must support AMD's SEV technology. To detect if the host hardware supports SEV, check that the `sev` attribute is in the capabilities of `libvirt` and that its value is set appropriately:

```
<domainCapabilities>
   ...
   <features>
   ...
   <sev supported='yes'/>
   ...
   </sev>
   </features>
</domainCapabilities>
```

Additionally, ensure that the `kvm_amd` kernel module has the `sev` parameter enabled:

```
/sys/module/kvm_amd/parameters/sev = 1
```

3 VM requirements

The VM must be the modern `Q35` machine type and must use UEFI firmware. `libvirt` can automatically select an appropriate SEV or SEV-ES enabled UEFI firmware, or one can be specified manually. Currently, the only firmware supported are `/usr/share/qemu/ovmf-x86_64-sev.bin` and `/usr/share/qemu/ovmf-x86_64-sev-code.bin`. See *Book "Virtualization Guide", Chapter 10 "Guest installation", Section 10.3.1 "Advanced UEFI configuration"* for more details on using UEFI firmware and the auto-selection feature.

> **Note: No IDE support in Q35**
>
> The Q35 machine type does not have an IDE controller and does not support IDE disks.

All `virtio-net` devices need to be configured with the iPXE option ROM disabled. iPXE is currently not compatible with SEV and SEV-ES. All memory regions used by the VM must be locked for Direct Memory Access (DMA) and to prevent swapping. This includes memory for the VM and any memory regions allocated by QEMU to support running the VM, such as UEFI pflash for firmware and variable store, video RAM, etc.

4 VM configuration

EXAMPLE 1: SAMPLE CONFIGURATION FILE

> As an example, an SEV-encrypted VM configured with 4 GB of memory would contain the following XML configuration:
>
> ```
> <domain type='kvm'>
>     <memory unit='KiB'>4194304</memory>
>     <currentMemory unit='KiB'>4194304</currentMemory>
>     <memoryBacking>
>     <locked/> ❶
>     </memoryBacking>
> ```

```
    <os>
    <type arch='x86_64' machine='pc-q35-2.11'>hvm</type>
    <loader readonly='yes' stateless='yes' type='pflash'>/usr/share/qemu/ovmf-
x86_64-sev.bin</loader>
    <boot dev='hd'/>
    </os>
    <launchSecurity ❷ type='sev'>
    <cbitpos>47</cbitpos> ❸
    <reducedPhysBits>1</reducedPhysBits> ❹
    <policy>0x0033</policy> ❺
    <dhCert>AAAABBBB=CCCCCDDDDD</dhCert> ❻
    <session>AAAABBBB=EEEEEFFFFF</session> ❼
    </launchSecurity>
    <devices>
    <interface type='bridge'>
    <source bridge='br0'/>
    <model type='virtio'/>
    <rom enabled='no'/> ❽
    </interface>
    ...
    </devices>
    ...
    </domain>
```

❶ The `memoryBacking` element, along with its child element `locking`, is used to ease memory limit restrictions `libvirt` places on the VM's cgroup. Otherwise, VM creation would fail when QEMU attempts to lock the VM's memory regions along with other regions used to support the VM operation. See https://libvirt.org/kbase/launch_security_sev.html#memory ↗ for more information on VM memory configuration requirements for SEV VMs.

❷ The `launchSecurity type='sev'` element and its contents enable encryption of the VM's memory contents.

❸ When memory encryption is enabled, one of the physical address bits (also known as the "C-bit") is used to mark if a memory page is protected. The required `cbitpos` element provides the location of the C-bit in a guest page table entry. For example, the value `47` indicates that bit position 47 in a page table entry determines whether that page is encrypted or not. The C-bit number is read from the host's CPUID and is thus hardware-dependent. The value of `cbitpos` is hypervisor-dependent, and can be obtained through the `sev` element in the capabilities of the domain.

④ When memory encryption is enabled, we lose certain bits of the physical address space. The required `reducedPhysBits` element provides this physical address bit reduction. Similarly to `cbitpos`, the value of `reducedPhysBits` is processor-family-dependent and can be obtained through the `sev` element in the domain capabilities.

⑤ The required `policy` element provides the guest policy which must be maintained by the SEV firmware. This policy is enforced by the firmware, and restricts what configuration and operational commands can be performed on the VM by the hypervisor. The guest policy provided when starting the VM is bound to that VM and cannot be changed throughout its lifetime.

⑥ The optional `dhCert` element provides the guest owner's base64-encoded Diffie-Hellman (DH) key. The key is used to negotiate a master secret key between the SEV firmware and guest owner. This master secret key is then used to establish a trusted channel between the SEV firmware and guest owner.

⑦ The optional `session` element provides the guest owner's base64-encoded session blob, as defined in the SEV API specification. See the LAUNCH_START section of the SEV specification for the session-blob format.

⑧ Besides the `launchSecurity` settings, SEV-encrypted VMs must have the iPXE option ROM disabled on all virtio-net devices. Currently, iPXE is not compatible with SEV-encrypted VMs.

The guest policy is four unsigned bytes with the following definition:

TABLE 1: GUEST POLICY DEFINITIONS

Bits	Definition
0	If set, debugging of the guest is disallowed
1	If set, sharing keys with other guests is disallowed
2	If set, SEV-ES is required
3	If set, sending the guest to another platform is disallowed
4	If set, the guest must not be transmitted to another platform that is not in the domain

Bits	Definition
5	If set, the guest must not be transmitted to another platform that is not SEV-capable
6-15	Reserved
16-32	The guest must not be transmitted to another platform with a lower firmware version

5 VM installation

virt-install supports the installation of SEV and SEV-ES virtual machines. In addition to your standard installation parameters, provide **virt-install** with options to satisfy the VM requirements and the `--launchSecurity` option.

The following example starts a network installation of a SLES 15 SP4 virtual machine protected with SEV-ES.

```
  virt-install --name sles15sp4-sev-es --location http://192.168.0.1/install/sles15sp4/
x86_64 --disk size=20 --network=bridge=br0,model=virtio,rom.bar=off ❶ --vcpus 4
 --memory 4096 --noautoconsole --events on_reboot=destroy --machine q35 --memtune
 hard_limit=4563402 --launchSecurity sev,policy=0x07 ❷ --boot firmware=efi ❸ --vnc --
serial pty
```

❶ The iPXE option ROM is not compatible with SEV-encrypted VMs and must be disabled on all virtio-net devices. While `libvirt` supports disabling option ROMs using either the `enabled` or `bar` attributes of the `rom` element, virt-install only supports disabling option ROMs using the `bar` attribute.

❷ The `launchSecurity` option specifies the type and policy to be enforced by the SEV firmware. The policy setting is described in *Table 1, "Guest policy definitions"*.

❸ The `boot` option allows specifying many boot-related settings, including the firmware used by the virtual machine. Specifying a firmware type `efi` allows libvirt's firmware auto-selection feature to select an appropriate SEV capable firmware for the virtual machine.

6 VM attestation

VM attestation is the process of verifying that trusted software components are correctly instantiated on a trusted compute platform. The process typically involves starting a VM in a paused state, retrieving a launch measurement of the instantiated software components, verifying the measurement, then providing a disk password or other key to unlock the VM and resume the paused boot process. The launch measurement includes cryptographic artifacts provided by the VM owner, with the cryptographic root of trust being the AMD SEV platform. The VM owner can be confident their software components have not been compromised and are running on a trusted platform once the launch measurement has been verified.

The overall attestation process is moderately complex with plenty of opportunity for error. Care must be taken to ensure the process itself is secure. For example, a secure attestation process cannot be executed directly on the hypervisor running the VM, since the goal is to demonstrate the hypervisor has not acted maliciously and contaminated the VM.

Although all the information and APIs required for attestation exist in SLES 15 SP4, SLES 15 SP5 introduces a simple utility called `virt-qemu-sev-validate` that can be used to satisfy several attestation use cases. For example, automated tests in quality assurance and small `libvirt` + KVM deployments that are not managed by large, commercial management stacks.

`virt-qemu-sev-vailidate` is included in the `libvirt-client-qemu` package and supports both offline and online attestation modes. `virt-qemu-sev-validate` requires all input for attestation as command-line parameters. Assuming it is invoked on a trusted machine, the results of `virt-qemu-sev-validate` can be trusted since no information is retrieved from untrusted sources. Online mode is less secure, particularly when executed directly on the hypervisor running the VM.

Regardless of mode, the attestation process of a `libvirt` + KVM VM starts with creating a VM or Guest Owner (GO) certificate and session blob that is unique for each start of the VM. The certificate and blob can be created with the `sevctl` utility, available in the `sevctl` package. The following example illustrates the use of the `sevctl session` command to create all the prelaunch SEV-related artifacts. The *NAME* parameter is optional and allows a prefix to be specified for the artifact file names. Using the VM name as a prefix is convenient for matching artifacts with VMs later. The path to the platform Diffie-Hellman (DH) certificate and the desired SEV policy are required parameters.

```
# sevctl session --name test-sev /data/sev/pdh.cert 7
```

The `sevctl session` command produces four files: tik.bin, tek.bin, godh.b64 and session.b64. If the optional *NAME* parameter was used, the files are prefixed with the specified value. The transport integrity key (tik.bin) and transport encryption key (tek.bin) are used in the verification stage of the attestation process. The guest owner Diffie-Hellman key (godh.b64) and session blob (session.b64) are copied to the VM XML configuration before starting the VM. See the `dhCert` and `session` subelements of the `launchSecurity` element in the VM configuration section for more details.

After the VM session artifacts have been created and VM XML configuration updated, the VM can be started in a paused state, for example:

```
# virsh -c qemu+ssh://USER_NAME@HOST_NAME/system create --paused /path/to/vm.xml
```

Creating the VM in a paused state allows retrieving the launch measurement from the hypervisor and comparing it to a measurement calculated on a trusted host using trusted inputs. If the measurements compare, the VM owner can be confident the VM has been properly instantiated on the hypervisor and execution can safely be started. The following command demonstrates using the `virsh domlaunchsecinfo` command to retrieve the paused VM launch measurement and other SEV-related information from the hosting hypervisor.

```
# virsh -c qemu+ssh://username@hostname/system domlaunchsecinfo sevtest
sev-measurement: VZjxMSlu+UuYkWHN2mAxDVVYXRmL3wqTu84kwk+5QS+4OMii7hs6cMAmXNpmmyS/
sev-api-major  : 1
sev-api-minor  : 51
sev-build-id   : 3
sev-policy     : 7
```

The retrieved launch measurement can then be given to `virt-qemu-sev-validate` to verify the VM has been securely instantiated. The following example demonstrates a full offline attestation of the measurement.

```
# virt-qemu-sev-validate --api-major 1 --api-minor 51 --build-id 3 --policy 7 \
 --firmware /usr/share/qemu/ovmf-x86_64-sev.bin --tik sevtest_tik.bin --tek
 sevtest_tek.bin --num-cpus 4 \
 --cpu-family 25 --cpu-model 1 --cpu-stepping 1 \
 --measurement QJ0oDpFmWj+bGZzFoMPbAxTuC6QD44W5w88x/hQM8toVsB75ci7V1YDfYoI9GTk
```

It is also possible to use **virt-qemu-sev-validate** in an online mode, where information needed to perform the VM attestation is retrieved from the hosting hypervisor. The following example demonstrates an online attestation of the VM, where only the hosting hypervisor URI, VM name, and associated TIK and TEK are specified. **virt-qemu-sev-validate** retrieves the remaining information, including the measurement itself, from the hosting hypervisor:

```
# virt-qemu-sev-validate --tik sevtest_tik.bin --tek sevtest_tek.bin \
  --connect qemu+ssh://USER_NAME@HOST_NAME/system --domain sevtest
```

Once the VM launch measurement has been verified, the VM owner can optionally inject a secret in the VM and resume VM execution. An example of injecting a secret would be providing a key to unlock an encrypted root disk.

```
# virsh -c qemu+ssh://USER_NAME@HOST_NAME/system domsetlaunchsecstate sevtest \
  --secrethdr hdr-str --secret secret-str
# virsh -c qemu+ssh://USER_NAME@HOST_NAME/system resume sevtest
```

7   SEV with KubeVirt

KubeVirt supports running SEV guests starting from the version `0.49.0`. The functionality can be activated by enabling the `WorkloadEncryptionSEV` feature gate:

```
> kubectl edit kubevirt kubevirt -n kubevirt
[...]
spec:
  configuration:
    developerConfiguration:
      featureGates:
      - WorkloadEncryptionSEV
[...]
```

To run an SEV-encrypted guest, the virtual machine specification must include the entry `sev: {}` under the `launchSecurity` domain element. Additionally, you need to configure the `firmware/bootloader` parameters to use the `efi` option with the `secureBoot` flag set to `disabled`. The corresponding YAML snippet looks similar to the following:

```
[...]
spec:
  domain:
    firmware:
      bootloader:
        efi:
          secureBoot: false
```

```
    launchSecurity:
      sev: {}
[...]
```

8 Current limitations

SUSE does not recommend using the SEV and SEV-ES features with SUSE Linux products on the first generation AMD EPYC™ 7000 series of processors, code name Naples. It is recommended to use at least the second generation 7002 series processors, code name Rome. Additionally, the following limitations are placed on SEV and SEV-ES VMs.

- The guest operating system running inside an SEV-encrypted VM must contain SEV support. SUSE Linux Enterprise Server 12 SP4 and newer, and all SUSE Linux Enterprise Server 15 releases support SEV.

- Any operations that involve saving and restoring the memory and state of an instance are currently not supported. This means that SEV-encrypted VMs cannot be resumed from snapshots, saved/restored, or live migrated. Encrypted VMs can be shutdown and restarted on another host as normal.

- SEV-encrypted VMs cannot contain directly accessible host devices (that is, PCI passthrough).

- SEV-encrypted VMs are not compatible with Secure Boot. UEFI firmware containing Secure Boot support does not work with SEV or SEV-ES VMs.

- SEV-ES VMs cannot be rebooted from within using `reboot`, `shutdown -r now`, etc. A reboot must be done by shutting down the VM and starting it again. This limitation does not apply to SEV VMs, only SEV-ES.

These limitations will be removed in the future as the hardware, firmware and specific layers of software receive new features.

9 More information

- https://developer.amd.com/sev ↗ — AMD-SEV landing page

- AMD SEV-KM API Specification (PDF) (https://www.amd.com/system/files/TechDocs/55766_SEV-KM_API_Specification.pdf) ↗

- AMD SEV GitHub repository containing examples and tools (https://github.com/AMDESE/AMDSEV/) ↗

- libvirt SEV configuration settings (https://libvirt.org/formatdomain.html#sev) ↗

- `libvirt` knowledge base article on AMD SEV (https://libvirt.org/kbase/launch_security_sev.html) ↗

10 Legal notice

Copyright© 2006– 2024 SUSE LLC and contributors. All rights reserved.

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or (at your option) version 1.3; with the Invariant Section being this copyright notice and license. A copy of the license version 1.2 is included in the section entitled "GNU Free Documentation License".

For SUSE trademarks, see https://www.suse.com/company/legal/ ↗. All other third-party trademarks are the property of their respective owners. Trademark symbols (®, ™ etc.) denote trademarks of SUSE and its affiliates. Asterisks (*) denote third-party trademarks.

All information found in this book has been compiled with utmost attention to detail. However, this does not guarantee complete accuracy. Neither SUSE LLC, its affiliates, the authors, nor the translators shall be held liable for possible errors or the consequences thereof.

GNU Free Documentation License

Copyright (C) 2000, 2001, 2002 Free Software Foundation, Inc. 51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA. Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

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.