GNU Boot manual (version 0.1-rc5)

GNU Boot Contributors (gnuboot@gnu.org)

Table of Contents

1 Overview 1

1.1 What is GNU Boot 1
1.1.1 boot software 1
1.1.2 distribution 3
1.2 Why free boot software is important 3
1.3 Why use GNU Boot 3
1.4 Other free boot software distributions 4
1.5 How much free software is GNU Boot? 4
1.6 Limitations 4

2 Supported hardware and configurations 6

2.1 Supported computers 6
2.2 Supported computer parts and peripherals 7
2.2.1 Supported GPUs and graphics 7
2.2.2 Supported card readers 8
2.2.3 Unsupported hardware supported by projects reused by GNU Boot 8
2.2.4 Supported operating systems 8
2.3 GNU Boot images 9
2.3.1 GNU Boot images types 9
2.3.2 GNU Boot images naming 10

3 Installing or upgrading GNU Boot images ... 12

3.1 Installation and upgrade instructions 12

4 Using GNU Boot 13

4.1 Using GNU Boot with QEMU 13
4.2 Security features 13

5 Building GNU Boot from source 15

5.1 Authenticating the GNU Boot source code 15

6 Helping GNU Boot 17

Appendix A GNU Free Documentation License .. 18

Concept index 26

1 Overview

This chapter will explain what is GNU Boot, and how it compares with somewhat similar projects.

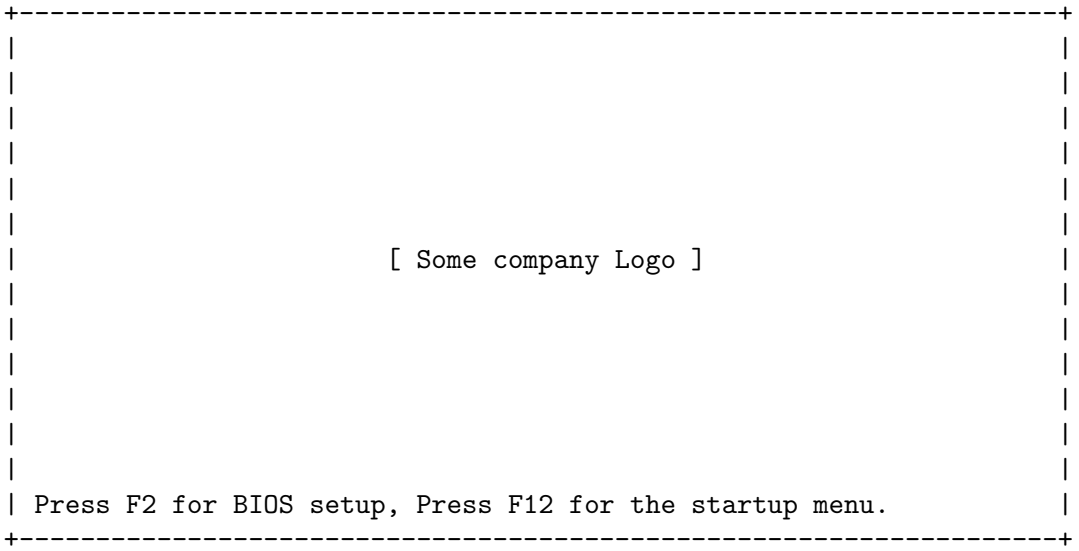
1.1 What is GNU Boot

GNU Boot is a boot software distribution. What this means will be explained below.

1.1.1 boot software

If you take a modern laptop computer, and remove the storage devices (like SSD (Solid State Drive), hard disks, etc) and then power on the computer, it will typically show something on the screen.

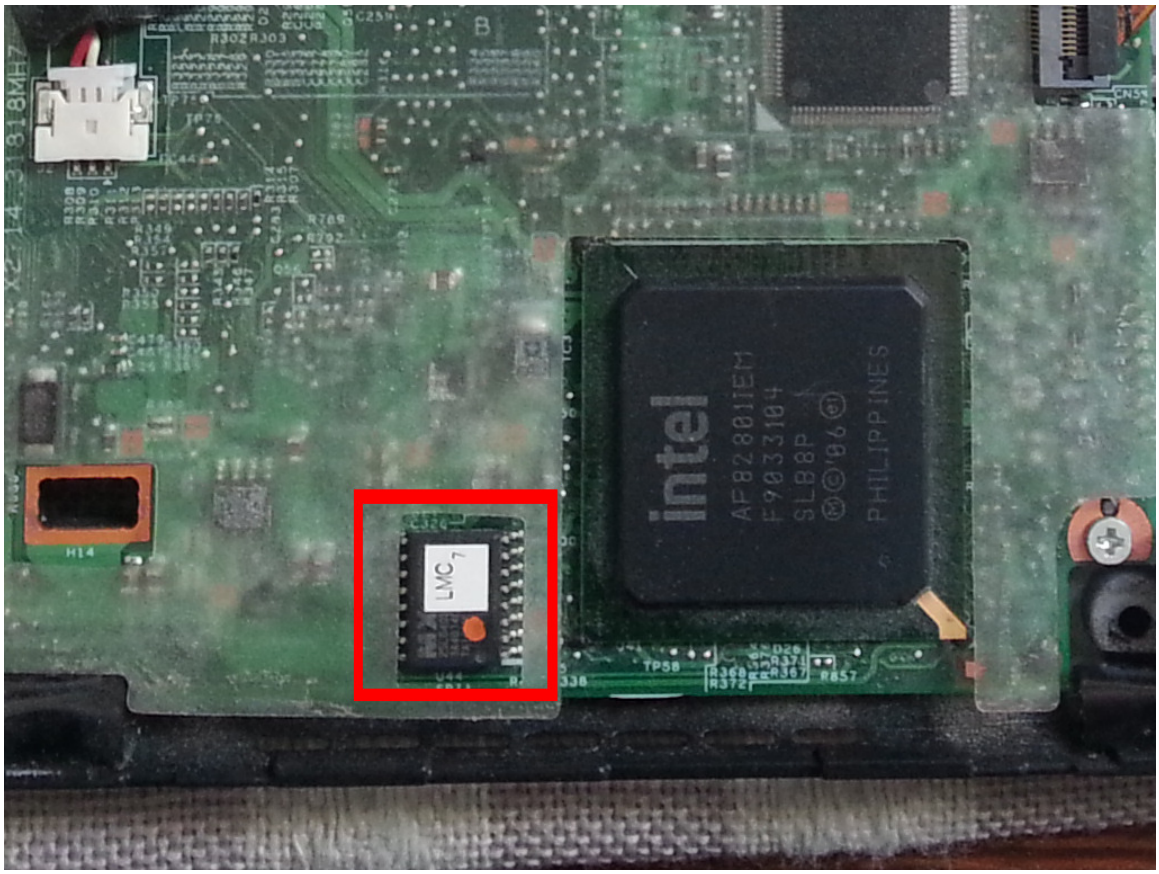
It often looks a bit like that:



What is being displayed on the screen is produced by software which is often nonfree.

It is often called BIOS (Basic Input/Output System) or UEFI (Unified Extensible Firmware Interface) on computers people are most familiar with. This software is typically stored inside a memory chip inside the computer mainboard. In some computers, this software can be replaced by free software.

Depending on how you read the manual, right below you may or may not see a picture of this memory chip on the mainboard of a ThinkPad X200.



The goal of this boot software is to initialize the hardware and load an operating system (like GNU/Linux).

This kind of "boot software" exists for a variety of reasons:

- The operating systems require certain hardware components like the RAM (Random Access Memory) to already work when they are started.
- The operating system is stored on a storage device(s) (like SSD (Solid State Drive), hard disks, etc) and part of it needs to be loaded inside the RAM (Random Access Memory) to work. Something has to do the loading, and this is done in software for flexibility and/or efficiency reasons.
- Finally, certain hardware components cannot be auto-detected and something needs to tell the operating system what drivers to load, which which settings.

GNU Boot provides such software. It enables to replace nonfree boot software (typically nonfree BIOS (Basic Input/Output System) or UEFI (Unified Extensible Firmware Interface)) on some computers.

1.1.2 distribution

GNU Boot is only a distribution because it reuses various software to produce something that can be installed.

So it is similar to GNU/Linux distributions like Trisquel 11 (aramo) that also reuse various software to produce something that can be installed.

1.2 Why free boot software is important

Freedom is important in general, and running nonfree software has negative consequences regardless of the type of software (game, boot software, operating system, driver, etc).

Here are some examples of common issues for nonfree boot software:

- Since the boot software loads the operating system, it can potentially modify it in a malicious way. In most cases part of the boot software also continues to run once the operating system is started. Because of that and, and because of the way the hardware and boot software run, the boot software can also do such modification at any time. If the boot software is nonfree, it is way harder to find and remove malicious code (it's even impossible to remove in some cases), and there is no way to make sure that there is none left. For instance many nonfree boot software where shipped with the CompuTrace malware (which was advertised as an anti-theft security feature).
- Vendors of various hardware components have to collaborate together to provide updates for nonfree Boot software, so in practice they decide when updates are done. So if a computer is not sold anymore, it is unlikely to get update for its Boot software unless the Boot software uses some free software that can be updated. Also note that applying nonfree updates comes with huge risk as we don't know what's inside the updates. Hardware vendors who provide the updates also have an incentive to make things worse for the users, so they would be pushed to buy new devices.
- Some nonfree Boot software restrict what you can do with your computer. For instance they refuse to boot if you changed or removed some hardware components.

1.3 Why use GNU Boot

As explained before GNU boot is just a distribution. So it is also possible to take the same software that GNU Boot reuses, and to build, assemble and install it yourself.

However doing that is risky because if something goes wrong, your computer won't boot anymore.

So the goals of GNU Boot are to:

- Collaborate together to test if GNU Boot releases works fine.
- Provide documentation to enable easy installation and usage.
- Limit the amount of work done by GNU Boot and contribute directly to the software we reuse whenever possible.

GNU Boot also has a long term focus, so it tries not to break users use cases, and tries as much as possible to fix issues in the projects it reuses instead of doing workarounds that impact users.

1.4 Other free boot software distributions

The following GNU/Linux distributions should also provide 100% free boot software but they usually only provide them for computers using the ARM architecture (which GNU Boot doesn't support yet):

- Parabola
- PureOS
- Trisquel

The GNU Guix package manager (which GNU Boot also reuses) also provide 100% free boot software for some ARM computers. However the Guix packages are updated all the time and the Guix project doesn't provide any way for users to report that specific ARM computers work fine with the boot software they provide.

There is also Canoeboot which is a 100% free software boot distribution similar to GNU Boot. Its goal is to remove nonfree software from Libreboot. It focuses more on having the latest software and many features, including some that are not available in the projects it reuses. Because of that it can be harder for users to use.

1.5 How much free software is GNU Boot?

Being a GNU package, GNU Boot itself is 100% free software. If you find nonfree software in GNU Boot and/or any source code or binaries released by GNU Boot, please contact its maintainers by opening a bug report on its bug tracker at `https://savannah.gnu.org/bugs/?group=gnuboot`.

But that doesn't mean that GNU Boot magically makes everything not provided by GNU Boot free software.

In some cases GNU Boot even runs nonfree software not provided by GNU Boot like nonfree GPUs drivers provided by the removable GPU card. See Section 2.2 [Supported computer parts and peripherals], page 7, for more details about this issue and how to avoid running such nonfree software.

To address problems like that the Free Software Foundation (`https://www.fsf.org/`) has created the Respect Your Freedom hardware certification (`https://ryf.fsf.org/`) to list hardware that works with only free software (with some very small exceptions for some components, see its criteria (`https://ryf.fsf.org/about/criteria`) for more details).

In addition there is also The Blob Fallacy article (`https://www.fsfla.org/ikiwiki/blogs/lxo/draft/blob-fallacy`) or a video of a presentation about the same issue at LibrePlanet 2024 (`https://media.libreplanet.org/u/libreplanet/m/software-enshittification-or-freedom-it-s-not-a-hard-choice`) by Alexandre Oliva that explains the related freedom issues with nonfree software provided by the hardware and how they compare with other kind of freedom issues (nonfree driver, nonfree firmware loaded automatically by Linux, etc).

1.6 Limitations

GNU Boot is fairly recent and doesn't have an official release yet.

For the release we plan to have at least some install and upgrade instructions for some computers and an easy way for users to use GNU Boot.

Also the latest GNU Boot release candidate was not tested yet with all the computers it's supposed to support (we badly need help for that).

2 Supported hardware and configurations

2.1 Supported computers

For now, GNU Boot only provides images that can be installed on the following computers:

- Acer G43T-AM3
- Apple MacBook 1.1
- Apple MacBook 2.1
- Apple iMac 5,2
- Asus KCMA-D8
- Asus KFSN4-DRE
- Asus KGPE-D16
- Gigabyte D945GCLF2D
- Gigabyte GA-G41M-ES2L
- Intel D410PT
- Intel D510MO
- Intel D945GCLF
- Lenovo ThinkPad R400
- Lenovo ThinkPad R500
- Lenovo ThinkPad T400
- Lenovo ThinkPad T400S
- Lenovo ThinkPad T500
- Lenovo ThinkPad T60 with intel GPU
- Lenovo ThinkPad W500
- Lenovo ThinkPad X200
- Lenovo ThinkPad X200S
- Lenovo ThinkPad X200T
- Lenovo ThinkPad X301
- Lenovo ThinkPad X60
- Lenovo ThinkPad X60T
- Lenovo ThinkPad X60s
- Libiquity Taurinus X200
- Qemu PC (i440FX)
- Technoethical D16
- Technoethical T400
- Technoethical T400s
- Technoethical T500
- Technoethical X200
- Technoethical X200s

- Technoethical X200 Tablet (X200T)
- Vikings ASUS KCMA D8 mainboard and workstation
- Vikings ASUS KGPE D16 mainboard
- Vikings X200

However as GNU Boot is still relatively new, we lack installation and upgrade instructions for most of these computers.

Also not all are well tested, so it's a good idea to look on the GNU Boot website, on the status page (`https://www.gnu.org/software/gnuboot/web/status.html`) for up to date result of tests by GNU Boot users and contributors.

2.2 Supported computer parts and peripherals

Most computer parts and peripherals don't have any compatibility issue with GNU Boot because:

- they either use some standard that is most often already implemented in the software GNU Boot reuses (storage devices like SATA drives, USB keyboards, etc),
- they are not relevant or supported for booting (for instance 3D printers, cellular network cards, etc, unless people add support for them in GNU Boot in the future). Until then they are only handled in the operating system instead (with drivers),

however there is some exceptions as some hardware is non-standard and still required for booting, these are documented in the subsections below.

2.2.1 Supported GPUs and graphics

GNU Boot supports the GPUs that are present in the various laptops it supports with 100% free software. Some consideration apply while booting (see Section 2.3 [GNU Boot images], page 9, for more details), but so far once booted these GPU are known to works well on tested computers.

In addition for the non-laptop computers, it also supports the builtin AST graphics in the KGPE-D16 and KCMA-D8 with 100% free software, but this also comes with some limitations: in GNU/Linux it's only possible to display text but not images, so it's limited to console applications.

In the case of PCIe GPU / graphics cards, we don't know yet if it is possible to use them without running nonfree software.

If AMD, ATI, and Nvidia cards work under GNU Boot, it's because GNU Boot loaded and run the nonfree video BIOS that is present on the card.

It's possible to prevent the nonfree video BIOS from running and you can easily confirm that as the display will not work until the Linux driver is loaded.

The Free Software Foundation tech team has a wiki. In the disable option roms with cbfstool article (`https://savannah.gnu.org/maintenance/fsf/hardware/disable-option-roms-with-cbfstool/`), they explains how to do that.

And in the graphics cards article (`https://savannah.gnu.org/maintenance/fsf/hardware/graphics-cards/`) they also explain which GPU they tested.

However the Linux driver can also run nonfree software: All the current AMD, ATI, and Nvidia drivers have code to load and run (a different) initialization code provided on the card. For ATI and AMD cards the code that Linux runs is called AtomBIOS.

We don't know yet if there are cases where this code is not run (this would need to be tested by doing very simple modifications to the drivers, and the GNU Boot project also welcome help in this area).

2.2.2 Supported card readers

GNU Boot supports the builtin card reader of the following computers:

- Lenovo ThinkPad X200
- Lenovo ThinkPad X200S
- Lenovo ThinkPad X200T
- Libiquity Taurinus X200
- Technoethical X200
- Technoethical X200s
- Technoethical X200 Tablet (X200T)
- Vikings X200

It also supports some USB card readers that are viewed as mass-storage. With all that you can boot on an SD card a microSD card and it will be viewed like a mass storage USB key.

2.2.3 Unsupported hardware supported by projects reused by GNU Boot

The following hardware components are supported by software reused by GNU Boot, but support for them hasn't been enabled yet in GNU Boot:

- Serial ports.
- Software RAID cards: Some Silicon Image SIL3114 software RAID cards are supported by Coreboot but not enabled in GNU Boot.
- Network interfaces. Projects like iPXE has drivers for many network cards and even some Wifi cards typically used with the computers supported by GNU Boot and free distributions.
- Some printers that use serial ports could probably easily be supported once serial ports are working.

The GNU Boot project needs help to evaluate the impact of enabling these and welcome contributions in this area.

2.2.4 Supported operating systems

While GNU Boot should be able to boot almost any GNU/Linux distribution, but in some cases some configuration might be needed by the GNU Boot user. The cases that do and don't require configuration from the user will be documented in Section 2.3 [GNU Boot images], page 9, below.

Even if some cases require some configuration, GNU Boot makes sure to provide at least one way to boot free GNU/Linux distributions (see `https://www.gnu.org/distros/` for

more information on these distributions) without the need to configure anything in order to make it possible for less technical users to use computers with GNU Boot, and even reinstall the GNU/Linux distribution without needing to do anything too complicated.

To make that possible, the GNU Boot contributors that proposes improvements to the project typically test GNU Boot with free distributions, and the GNU Boot project even runs automatic tests with Trisquel 11 (aramo), one of the free distributions to make sure that it can boot fine without needing any special configuration from the user.

However sometimes fully free distributions also propose experimental or non-standard configurations for very specific use cases. For instance Guix has experimental support for GNU Hurd, an experimental kernel from the GNU project, and Trisquel supports the Xen kernel, which is a virtualization solution that not supported by all GNU/Linux distributions. These configurations are not supported in the official installers of these distribution and so users are usually aware thaty they use Xen or GNU Hurd. Using GNU Boot with these configurations might require some configuration from the user. Also we would need help from users to report what works and doesn't work or what workarounds are needed to make them work with GNU Boot.

The cases that are known not to require any configuration might also work with any GNU/Linux distributions (even the nonfree ones), however the GNU Boot project doesn't want to force contributors to download or run nonfree software to test changes, so it relies on voulounteers already running such distributions to report bugs in case something doesn't work as it should.

As for other operating systems, there is some documentation on how to boot some of them (like some BSD operating systems) on the GNU Boot website, but again we need help from voulonteers already running such systems to keep the documentation up to date and inform us of what works and doesn't work.

Also if you want to do such tests, you can open a bug report on the GNU Boot bug tracker at `https://savannah.gnu.org/bugs/?group=gnuboot`.

2.3 GNU Boot images

In computers people are most familar with, like laptops, the boot software resides in a memory chip inside the mainboard (see Section 1.1.1 [boot software], page 1, for more details).

GNU Boot provide *image files* which are files that replace the content of these memory chip.

These files are similar to disk images (`https://en.wikipedia.org/wiki/Disk_image`), ISO images (`https://en.wikipedia.org/wiki/ISO_image`), or ROM images (`https://en.wikipedia.org/wiki/ROM_image`).

We also sometime refer to the flash image files as *flash images*.

2.3.1 GNU Boot images types

For a given computer, GNU Boot provides several images with different software in it. This enable the users to choose between:

- Two boot software: GRUB or SeaBIOS (BIOS (Basic Input/Output System) implementation)

- Various keyboard layouts (colemak, deqwertz, esqwerty, frazerty, frdvbepo, itqwerty, svenska, trqwerty, ukdvorak, ukqwerty, usdvorak, usqwerty).
- Low resolution or high resolution graphics.

If you are a less technical user or helping one, or don't have much time to configure things, it is a good idea to choose an image with GRUB, and a keyboard layout of your choice (the resolution is not very important, but using high resolution looks nicer) as the image with GRUB doesn't require to do any configuration in the distributions you want to boot.

Otherwise here are the advantages/disadvantages of each combinaison:

- GRUB with high resolution graphics: Images with GRUB usually don't require the user to do any configuration of the distribution. More technical users can also use that to customize the way the system boots for more security or to support unsual boot configurations (that are not typically supported by graphical installers of GNU/Linux distributions), however these more advanced configurations also come with their set of limitations.
- SeaBIOS with text-only low resolution: It implements BIOS (Basic Input/Output System) compatibility, so it is very similar to a nonfree BIOS (Basic Input/Output System) but it require users to modify some settings inside the distribution they use, otherwise the distribution still boots but usually has a black screen during the boot (which can be problematic to diagnose a non-booting distribution). The low resolution increase compatibility with various software that are typically run at boot like memtest86+ (a software that detects broken RAM chips).
- GRUB with text-only low resolution: Since these images boot with GRUB, they also don't require any configuration of the distribution and more technical users can also use them to customize the way the system boots. Compared to GRUB images with high resolution graphics:
  - the text is bigger and that there is no background picture
  - since on most supported computers, GRUB images can also load and run SeaBIOS (there is a menu entry for it), having a text-only low resolution increase the compatibility with various boot software.
- SeaBIOS with high resolution graphics:

  Since these images boot with SeaBIOS they also implement some BIOS (Basic Input/Output System) compatibility, but they also require users to modify some settings inside the distribution they use. Compared with SeaBIOS images with text-only low resolution:
  - they are less compatible with various boot software. This can be useful for testing if you contribute to some boot software.
  - since on most supported computers, SeaBIOS images can also load and run GRUB (there is a menu entry for it when pressing the 'ESC' key at boot), having high resolution graphics can make GRUB look nicer.

2.3.2 GNU Boot images naming

Images for specific computers can be found on the GNU Boot download area (`https://ftp.gnu.org/gnu/gnuboot/`) or in the release/roms directory if you built GNU Boot from source yourself.

For a given release (or release candidate) like GNU Boot 0.1-rc3, you can find such files inside the 'roms' directory like `https://ftp.gnu.org/gnu/gnuboot/gnuboot-0.1-rc3/roms/` for GNU Boot 0.1-rc3.

Inside you have archive files like `gnuboot-0.1-rc3_x200_8mb.tar.xz` that are specific to a specific computer (here the ThinkPad X200 with 8MiB flash chip).

see Chapter 3 [Installing or upgrading GNU Boot images], page 12, to understand how to identify which archive file correspond to which computer.

Inside each archive files, there are many smaller files that are flash images. See Section 1.1.1 [boot software], page 1, to understand what a flash image is.

The flash image files correspond to the configurations described in the Section 2.3.1 [GNU Boot images types], page 9.

So for instance if we have an image named `grub_x200_8mb_corebootfb_usqwerty.rom`, it is meant for a ThinkPad X200 with 8MiB flash chip, and it uses the GRUB software to boot, and it is configured to use a QWERTY keyboard layout.

If the image contains `seabios` in its file name instead of `grub`, it uses the SeaBIOS software to boot.

The `corebootfb` in the file name correspond to the high resolution graphics described in the previous subsection (Section 2.3.1 [GNU Boot images types], page 9).

If instead the file has `txtmode` in its name, this corresponds to the text-only low resolution that was also described in the previous subsection (Section 2.3.1 [GNU Boot images types], page 9).

3 Installing or upgrading GNU Boot images

GNU Boot provides flash images for specific computers that can be found on the GNU Boot download area (https:// ftp.gnu.org/gnu/gnuboot/).

But depending on your threat model, it could be a good idea to build GNU Boot from source yourself instead, to avoid certain security attacks. See Section 4.2 [Security features], page 13, section for more context with security and threat models and Chapter 5 [Building GNU Boot from source], page 15, for more details about the security attacks mentioned above.

Once GNU Boot is downloaded or built, you will need to understand which files you need to install or upgrade. See Chapter 2 [Supported hardware and configurations], page 6, chapter for more details on how to do that.

3.1 Installation and upgrade instructions

The GNU Boot manual doesn't have well integrated installation or upgrade instructions yet but some generic installation and upgrade instructions can be found in the GNU Boot website. We need help to migrate these instructions in the manual and make them easier to understand.

4 Using GNU Boot

4.1 Using GNU Boot with QEMU

The GNU Boot project also release images for QEMU.

If you just want to try an image to see how it looks like you can use the following command:

```
qemu-system-x86_64 -M pc \
-bios grub_qemu-pc_2mb_corebootfb_usqwerty.rom
```

Here you need to replace *grub_qemu-pc_2mb_corebootfb_usqwerty.rom* by the path to the image you want to try.

For a more complete example, you can look in the GNU Boot source code as GNU Boot uses QEMU to run some automatic tests that boots Trisquel 11 (aramo).

Also note that the GNU Boot images for QEMU can be useful in some situations, but it doesn't fully replace tests run on real computers.

For instance a distribution or operating system might work on QEMU but not work on real hardware due to an incomplete graphic driver for the real hardware GPU.

4.2 Security features

Note that security is a process. To really make it work you need to understand various threats and how to respond to them (this is called *threat modelling*), so what security feature to use or not to use depends on your life, use cases, etc.

Also note that in general some security features also have downsides, such as making it harder to use the computer, making it harder to fix issues, etc, so not everybody might want these security features.

As for security features typically found in other boot software, some computers vendor sell computers with what they call *secure boot*. When it cannot be turned off, it becomes an anti-feature and the Free Software Foundation (`https://www.fsf.org/`) calls it *restricted boot*.

In 2012, the Free Software Foundation (`https://www.fsf.org/`) wrote a whitepaper (`https://www.fsf.org/campaigns/secure-boot-vs-restricted-boot/campaigns/secure-boot-vs-restricted-boot/whitepaper.pdf`), on the topic and advised that:

```
The best solution currently available for operating system distributions
includes:
1. fully supporting user-generated keys, including providing tools and full
documentation for booting and installing both modified and official
versions of the distribution using this method;
2. using a GPLv3-covered bootloader to help protect users against the
dangers of Restricted Boot;
3. avoiding requiring or encouraging users to trust Microsoft or any com-
pany which makes proprietary software; and
4. joining the FSF and the broader free software movement in pressuring
computer distributors to facilitate easy and independent installation of
```

`free software operating systems on any computer.`

GNU Boot supports various security mechanism: GRUB is a GPLv3-covered bootloader that GNU Boot reuses, and it supports user-generated keys or other security mechanism that that don't require any signing keys.

GNU Boot also obviously doesn't Trust keys from companies that make proprietary software.

At the end when used correctly, the security features provided by GNU Boot thanks to the software it reuses (like GRUB) can provide similar or stronger security guarantees than the UEFI secure boot with different security features that you may or may not want want to use depending on your threat model.

The GNU Boot Website contains various information on how to use such security features, but they are also documented in the *GNU GRUB manual* as well in more details. Since the GRUB version GNU Boot uses might be older than the online GRUB manual, you can use Guix to install the manual of older GRUB versions (see *GNU Guix reference manual* for more details).

All the security mechanism described in the GRUB manual or GNU Boot website are compatible with users freedom.

5 Building GNU Boot from source

Currently building GNU Boot flash images on two different computers will produce slightly different images.

This is a problem as it prevents people from easily verifying that the official flash images really correspond to the source code published by GNU Boot, and having the ability for anyone to verify that increases the security guarantees.

The Reproducible builds (`https://reproducible-builds.org`) project helps publicizing this problem and helps distributions and software to fix it.

So while GNU Boot also started working to fix this problem the work just stated and isn't complete yet, so in the meantime if you care about this type of risks, it might be a good idea to build GNU Boot from source yourself.

The GNU Boot website has instructions for building GNU Boot at the following URL: `https://www.gnu.org/software/gnuboot/web/docs/build/`.

See Section 5.1 [Authenticating the GNU Boot source code], page 15, as GNU Boot has ways to prevent network attacks from tempering with the souce code you are downloading.

Note that at the moment, building GNU Boot from tarballs is unsupported, so you will have to download GNU Boot from git and build from git.

5.1 Authenticating the GNU Boot source code

As explained on the GNU Boot build instructions (`https://www.gnu.org/software/gnuboot/web/docs/build/`) on the GNU Boot website, to build GNU Boot you will need to install Guix first (it can be installed on top of another GNU/Linux distribution).

You can consult either the GNU Boot build instructions (`https://www.gnu.org/software/gnuboot/web/docs/build/`) or the Section "Installation" in *GNU Guix reference manual* for how to do that.

Once this is done you can download the GNU Boot source code with the following command and go into it:

```
$ git clone https://git.savannah.gnu.org/git/gnuboot.git
$ cd gnuboot
```

And you can then authenticate the source code with the following guix command:

```
$ guix git authenticate \
dde4223088cbfe8a347626638d32902ba2323b25 \
"E23C 26A5 DEEE C5FA 9CDD  D57A 57BC 26A3 6871 16F6" \
-k origin/keyring
```

It should then print the following text:

```
guix git: successfully authenticated commit dde4223088cbfe8a347626638d32902ba2323b25
```

See Section "Invoking guix git authenticate" in *GNU Guix manual* or the Authenticate your Git checkouts! Guix blog post (`https://guix.gnu.org/en/blog/2024/authenticate-your-git-checkouts/`) for more details.

The question that remains is then how to make sure that "E23C 26A5 DEEE C5FA 9CDD D57A 57BC 26A3 6871 16F6" is the right key.

To do that the GnuPG software can help (see *its manual* for now to use it if you are interested) but the solution to this problem is not technical but social and could require significant time and effort.

To solve this problem you will need to build some sort of chain of trust between you and the person who controls the "E23C 26A5 DEEE C5FA 9CDD D57A 57BC 26A3 6871 16F6" key (here Adrien 'neox' Bourmault) with or without the help of the GnuPG software.

Wikipedia has a bit more information on the problem in its Web of trust (`https://en.wikipedia.org/wiki/Web_of_trust`) article, and the The GNU Privacy Handbook (`https://www.gnupg.org/gph`) has a section about Building your web of trust (`https://www.gnupg.org/gph/en/manual/x547.html`), that contains advises on how to do that, especially in the part about "Key validation".

6 Helping GNU Boot

The GNU Boot project needs help with this manual, specifically on moving information from the GNU Boot website to this manual.

In general there is also a lot of ways to help the GNU Boot project (from reviewing website pages for very simple mistakes or outdated information, testing GNU Boot images, etc).

See the Helping GNU Boot (`https://www.gnu.org/software/gnuboot/web/git.html`) page on the GNU Boot website for the areas where we need help and on how to help practically speaking (how to contact the project, where to send bug reports, etc).

Appendix A GNU Free Documentation License

Version 1.3, 3 November 2008

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 in order 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.

The "publisher" means any person or entity that distributes copies of the Document to the public.

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 noncommercially, 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 under this License. Any attempt otherwise to copy, modify, sublicense, or distribute it is void, and will automatically terminate your rights under this License.

   However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

   Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

   Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, receipt of a copy of some or all of the same material does not give you any rights to use it.

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/licenses/`.

    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. If the Document specifies that a proxy can decide which future versions of this License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Document.

11. RELICENSING

    "Massive Multiauthor Collaboration Site" (or "MMC Site") means any World Wide Web server that publishes copyrightable works and also provides prominent facilities for anybody to edit those works. A public wiki that anybody can edit is an example of such a server. A "Massive Multiauthor Collaboration" (or "MMC") contained in the site means any set of copyrightable works thus published on the MMC site.

    "CC-BY-SA" means the Creative Commons Attribution-Share Alike 3.0 license published by Creative Commons Corporation, a not-for-profit corporation with a principal place of business in San Francisco, California, as well as future copyleft versions of that license published by that same organization.

    "Incorporate" means to publish or republish a Document, in whole or in part, as part of another Document.

    An MMC is "eligible for relicensing" if it is licensed under this License, and if all works that were first published under this License somewhere other than this MMC, and subsequently incorporated in whole or in part into the MMC, (1) had no cover texts or invariant sections, and (2) were thus incorporated prior to November 1, 2008.

    The operator of an MMC Site may republish an MMC contained in the site under CC-BY-SA on the same site at any time before August 1, 2009, provided the MMC is eligible for relicensing.

ADDENDUM: How to use this License for your documents

To use this License in a document you have written, include a copy of the License in the document and put the following copyright and license notices just after the title page:

```
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 1.3
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.

Concept index

B

BIOS (Basic Input/Output System) 1
boot software 1

F

flash images 9

I

image files 9

S

secure boot 13

T

threat modelling 13

U

UEFI (Unified Extensible Firmware Interface) 1