### Tails - Feature #6560
### UEFI Secure boot

#### Description
At some point, Tails will have to support UEFI Secure boot.

#### Team: FT

### Subtasks:
- Feature # 15806: Use GRUB for USB boot on EFI 64-bit
- Feature # 17494: Update design doc for GRUB + Secure Boot
- Bug # 17352: Release alpha with Secure Boot, GRUB, and overlayfs
- Feature # 17373: Tweet secure boot
- Feature # 17452: Figure out what to do with VirtualBox dkms modules vs. Secure Boot
- Feature # 17459: Triage user feedback wrt. Secure Boot alpha
- Feature # 17492: Update documentation wrt. using GRUB + Secure Boot for USB boot on EFI...
- Bug # 16229: Boot Loader Menu documentation does not support 32-bit UEFI
- Feature # 16410: Document how to allow macOS Startup Security Utility to boot on extern...
- Feature # 17538: Make it easy for users to identity whether they get GRUB or SYSLINUX

### Related issues:
- Related to Tails - Feature #11679: Rethink the installation process and upgra... Resolved 08/20/2016
- Related to Tails - Bug #15016: Explain better how to disable Secure Boot Rejected 12/05/2017
- Blocked by Tails - Feature #5739: Support UEFI boot Resolved 10/03/2013
- Blocked by Tails - Feature #15292: Distribute a USB image Resolved 04/14/2016 01/29/2019
- Blocked by Tails - Feature #8415: Migrate from aufs to overlayfs Resolved 12/18/2014
- Blocked by Tails - Feature #15944: Port Tails to Buster Resolved 09/12/2018
- Blocks Tails - Feature #16209: Core work: Foundations Team Confirmed
- Blocks Tails - Feature #17495: Run most of our test suite with Secure Boot en... Confirmed

### Associated revisions
**Revision 69157449 - 04/11/2019 11:33 AM - intrigeri**

Use GRUB with Secure Boot support for x86_64 (refs: #6560, #15806)

**Known limitations:**

- Until Debian's shim-signed is signed by Microsoft, this will only work after enrolling the Debian test signing key: [https://wiki.debian.org/SecureBoot/Testing](https://wiki.debian.org/SecureBoot/Testing)

- Until we switch to overlayfs, this won't boot as the out-of-tree aufs module is not signed and the kernel will thus refuse loading it when Secure Boot is enabled (#8415).
- No signed EFI binaries for ia32: shim-signed is only built for amd64 at the moment. Besides, grub-efi-ia32-signed is only available in the i386 Debian archive (which could be solved using APT's multiarch support).
This is out of scope for this project.

- Our design doc is outdated.

- The GRUB menu may be less user-friendly than the previous syslinux one.

- No background image in the GRUB menu; however, note that we had to disable the background image for syslinux in UEFI mode since it broke the bootloader on some hardware.

- Our test suite relies on syslinux (images, keystrokes).

Revision 6b48783f - 04/11/2019 12:52 PM - intrigeri

Make GRUB configuration compatible with Debian's Secure Boot implementation (refs: #6560)

With Secure Boot enabled, we can't load the (unsigned) syslinux.cfg and cpuid GRUB modules. So we need to write a self-sufficient GRUB configuration file ourselves, instead of loading the syslinux one.

Also, drop one layer of indirection:

- use /EFI/debian/grub.cfg, which is loaded by default by the Debian-signed GRUB EFI image

- install GRUB modules under /EFI/debian/grub, where the Debian-signed GRUB EFI image look for them by default

This avoids having to write extra code that would locate the actual place where the GRUB files, and set $root and $prefix accordingly, which might not even possible to do without trusting all local partitions.
Accordingly, set prefix to /efi/debian/grub when generating the unsigned GRUB image for 32-bit EFI.

Revision 3da2ff54 - 11/27/2019 05:25 PM - segfault
Display background image in GRUB (refs: #6560)

Revision 5d0ad3e4 - 11/27/2019 05:25 PM - segfault
Use the AMNESIA_APPEND variable in grub.cfg (refs: #6560)

Revision 4bf8cc24 - 11/27/2019 09:34 PM - segfault
Use a custom background image for GRUB (refs: #6560)

The syslinux boot menu is displayed in the center of the screen and in the background image we use for syslinux, we put the Tails logo on the left, so that it's displayed left of the boot menu.

The GRUB boot menu uses a bigger part of the screen. When using the same background image as for syslinux, the logo looks out of place.

This adds a custom background image for GRUB, in which the logo is in the center.

Revision 7a150c77 - 11/27/2019 09:45 PM - segfault
Set timeout for GRUB boot menu (refs: #6560)

To 4 seconds, same as for syslinux.

Revision c6c827bf - 02/21/2020 05:13 PM - intrigeri
Test suite: add a tag for UEFI-related scenarios (refs: #6560)

Revision e9e59d9b - 03/20/2020 09:01 AM - intrigeri
Manual test suite: fix typo (refs: #6560)

Revision 1f912dae - 03/20/2020 09:02 AM - intrigeri
Manual test suite: clarify how to recognize GRUB (refs: #6560)

It's written on the box :)

Revision fc3be717 - 03/20/2020 09:10 AM - intrigeri
Declare variables as local (refs: #6560)

Revision 7ca99d6f - 03/21/2020 06:27 PM - intrigeri
Merge branch 'feature/6560-secure-boot-force-all-tests' into devel (Closes: #6560, #8415, #15806, #17049)

History

05/18/2020
#1 - 01/02/2014 04:07 AM - intrigeri
- Category set to Hardware support

#2 - 01/02/2014 04:10 AM - intrigeri
- Priority changed from Normal to Low

#3 - 05/27/2014 10:59 AM - BitingBird
- Status changed from Confirmed to In Progress
- % Done changed from 0 to 10

There is a blueprint, so I change the status to "in progress"

#4 - 05/27/2014 11:11 AM - intrigeri
- Status changed from In Progress to Confirmed

BitingBird wrote:

There is a blueprint, so I change the status to "in progress"

Honestly, the blueprint is just a compilation of bookmarks we've collected in the last few years. We have no plan, no idea which one of the various main paths we'll pick, and nobody is actively working on it, nor has plans to do so. So, I don't think "In progress" reflects correctly the real state of this task, and I'd rather not see this indication discourage anyone from tackling it. (Oh, and next time you'll triage the "In progress without assignee" tickets, it would pop up on your radar again ;)

#5 - 07/16/2017 06:58 PM - zjaume
Would this feature implemented? I think it's very anoying to disable Secure Boot on every PC when trying to boot tails.

#6 - 02/03/2018 04:24 PM - intrigeri
- Related to Feature #11679: Rethink the installation process and upgrade process added

#7 - 02/06/2018 04:04 PM - intrigeri
- Blocked by Feature #15292: Distribute a USB image added

#8 - 08/17/2018 06:14 AM - intrigeri
- Related to Bug #15016: Explain better how to disable Secure Boot added

#9 - 08/17/2018 06:24 AM - intrigeri
It is now quite likely that Debian Buster will have Secure Boot support (see https://debconf18.debconf.org/talks/59-report-from-the-debian-efi-team-about-the-support-of-secure-boot-on-debian/ for the latest status update). According to the tracking bug, the only remaining blockers that matter for Tails are https://bugs.debian.org/821051 and https://bugs.debian.org/820050.

This will allow us to add such support to Tails, hopefully without too much trouble. We'll have to switch to GRUB2, at least for USB sticks; wrt. DVD boot, since the ISO will only be supported for VMs after #15292 is done, if it's cheaper the ISO can keep using isolinux and not support Secure Boot.
#10 - 08/18/2018 02:04 PM - intrigeri
- Blocked by Feature #15806: Use GRUB for USB boot on EFI 64-bit added

#11 - 09/14/2018 11:37 AM - intrigeri
- Description updated
- Priority changed from Low to Normal
- Target version set to 2019

#12 - 11/04/2018 04:23 AM - sajolida
Someone is doing this already by patching an already-installed Tails:


Could we do this as well?

(Updated link to archive: https://lists.autistici.org/message/20181104.032028.086db28c.en.html — which mostly points to https://pav-computer-notes.blogspot.com/2017/10/patching-tails-usb-stick-for-uefi.html -- intrigeri)

#13 - 11/05/2018 09:37 AM - intrigeri

Could we do this as well?

Replied on tails-dev. tl;dr: yes, if we postpone something else or find/hire more developers.

#14 - 11/06/2018 01:09 AM - sajolida

My learning from https://mailman.boum.org/pipermail/tails-dev/2018-November/thread.html is that support for Secure Boot is not blocked by Debian 10 (Buster).

#15 - 12/22/2018 06:20 PM - beta-tester

intrigeri wrote:

At some point, Tails will have to support UEFI Secure boot.

Team: FT

please don't forget those people who has a tablet/netbook with 64bit CPU but UEFI 32bit. those can't be booted with a bootx64.efi file. they need a bootia32.efi. the only distribution that provides those capability at the moment is Fedora 29 Workstation Live (64bit). and all bootia32.efi and bootx64.efi stuff there is "Microsoft Corporation UEFI CA" signed, to be able to UEFI boot with SecureBoot enabled.

see also https://bugs.launchpad.net/ubuntu/+source/shim-signed/+bug/1793994
please don't forget those people who has a tablet/netbook with 64bit CPU but UEFI 32bit.

We've supported these systems (with Secure Boot disabled) since Tails 1.5. I do hope we'll manage to add Secure Boot support for those too. Depending on how hard it is, we might or might not block on it.

**#17 - 01/12/2019 04:34 PM - intrigeri**
- Blocked by Feature #8415: Migrate from aufs to overlayfs added

**#18 - 01/12/2019 04:36 PM - intrigeri**

Blocked by Feature #8415: Migrate from aufs to overlayfs added

Explanation: due to the lockdown patches, the kernel will refuse loading unsigned modules, such as the aufs module we're building ourselves. So this ticket is blocked by #8415, which is itself blocked by #15281. It might be that the dependency tree is larger, let's make sure we have it in mind if/when we prepare a grant proposal for Secure Boot.

**#20 - 04/02/2019 03:26 PM - intrigeri**
- Blocked by Feature #15944: Port Tails to Buster added

**#21 - 04/05/2019 04:09 PM - intrigeri**
- Blocks Feature #16209: Core work: Foundations Team added

**#22 - 04/11/2019 01:58 PM - intrigeri**
- Status changed from Confirmed to In Progress

Applied in changeset tails/69157449b1d90b6f3fd170e4485b83c7134aa8f4.

**#23 - 04/11/2019 01:59 PM - intrigeri**
- Status changed from In Progress to Confirmed
- Feature Branch set to wip/feature/6560-secure-boot

Got a PoC that boots fine until the kernel refuses to load the aufs module, on a system with Secure Boot enabled.

**#24 - 09/13/2019 07:14 AM - intrigeri**
#25 - 11/27/2019 05:25 PM - segfault
- Status changed from Confirmed to In Progress

Applied in changeset tails|3da2ff54fc73abc8da1da170ba941406ae5cd09e.

#26 - 12/01/2019 11:24 AM - intrigeri
- Priority changed from Normal to High
- Target version changed from 2019 to Tails_4.5

Some of this has to be done by May, some of it by July.

#27 - 02/21/2020 03:24 PM - intrigeri
- Feature Branch changed from feature/6560-secure-boot to feature/6560-secure-boot+force-all-tests

#28 - 02/22/2020 07:22 AM - intrigeri
- Related to Feature #17492: Update documentation wrt. using GRUB + Secure Boot for USB boot on EFI 64-bit added

#29 - 02/23/2020 07:08 AM - intrigeri
- Blocks Feature #17495: Run most of our test suite with Secure Boot enabled added

#30 - 03/15/2020 03:43 PM - intrigeri
- Blocked by deleted (Feature #15806: Use GRUB for USB boot on EFI 64-bit)

#31 - 03/18/2020 02:51 PM - anonym
- Status changed from In Progress to Needs Validation
- Assignee set to anonym
- Feature Branch changed from feature/6560-secure-boot+force-all-tests to feature/6560-secure-boot+force-all-tests, https://salsa.debian.org/tails-team/tails/-/merge_requests/44/

I'll review this on GitLab, looking at the diff, not the commits (which stretch back to 2015! Eeek!).

#32 - 03/19/2020 05:31 PM - anonym
- Assignee changed from anonym to intrigeri

Woohoo! Great work, you two! I'm almost a bit unhappy with how little I had to remark about. :D Non of them are really blockers, IMHO.

So, I am in particular done with all the code, so I deem this merge-worthy, but I would like to give another pass to the changes of docs and automated tests (honestly, that linting commit made things harder for me, and I am very glad it was only applied to usb.rb), which I plan to do tomorrow (2020-03-20) morning. But I don't think you should block on this. So, at least from my PoV, feel free to go ahead and merge whenever you want.

#33 - 03/20/2020 08:53 AM - intrigeri
- Status changed from Needs Validation to In Progress

Hi @anonym,

Woohoo! Great work, you two! I'm almost a bit unhappy with how little I had to remark about. :D Non of them are really blockers, IMHO.

So, I am in particular done with all the code, so I deem this merge-worthy,
Sweet! Does this mean you agree #15146 is not a blocker, or did you miss it so far?

I'll look at your code review this morning and I should manage to push the corresponding follow-up commits today. Then I'll reassign to you for another review pass (without waiting for CI results).

honestly, that linting commit made things harder for me, and I am very glad it was only applied to usb.rb

Yeah, in retrospect I should have dropped that commit once I realized that the amount of changes needed to get a significant benefit (having the linting tool not disabling itself in my editor because of "too many problems, giving up!") was much bigger than I expected. Sorry for the burden!

And to put this into perspective, IMO this relates to the problem introduced with "We have a hard time balancing these aspects" in summit.git/WIP/Healing_our_community.mdwn: it was easier and more pleasurable for me to do this work while I was there, but it caused trouble for you.

Off-topic: I'd really like us to have coding standards, ideally not too far from established Ruby best practices. So I'll try to come back to this and do a PoC mass linting in a dedicated branch. Then we can decide how much we value personal preferences over established best practices, which may result in disabling some of the linting rules in a config file in Git, so everyone's brain/editor/IDE/linter can be aware of our coding standards.

So, at least from my PoV, feel free to go ahead and merge whenever you want.

FTR, before merging I'll block on:

- One of anonym & segfault commenting on #15146
- kibi's "what can possibly go wrong" input

---

#34 - 03/20/2020 09:18 AM - intrigeri
- Status changed from In Progress to Needs Validation
- Assignee changed from intrigeri to anonym
I'll look at your code review this morning and I should manage to push the corresponding follow-up commits today. Then I'll reassign to you for another review pass (without waiting for CI results).

Done! (I'll monitor CI results.)

---

#35 - 03/20/2020 09:36 AM - anonym
intrigeri wrote:

Hi anonym,

Woohoo! Great work, you two! I'm almost a bit unhappy with how little I had to remark about. :D Non of them are really blockers, IMHO. So, I am in particular done with all the code, so I deem this merge-worthy,

Sweet! Does this mean you agree #15146 is not a blocker, or did you miss it so far?

Gah, I had forgotten to click the "Submit" button for the post I wrote yesterday. But yes, #15146 is not a blocker, IMHO.

I'll look at your code review this morning and I should manage to push the corresponding follow-up commits today. Then I'll reassign to you for another review pass (without waiting for CI results).

Ack! I'll also do another pass on the docs and tests, as I said yesterday.

honestly, that linting commit made things harder for me, and I am very glad it was only applied to usb.rb

Yeah, in retrospect I should have dropped that commit once I realized that the amount of changes needed to get a significant benefit (having the linting tool not disabling itself in my editor because of "too many problems, giving up!") was much bigger than I expected. Sorry for the burden!

And to put this into perspective, IMO this relates to the problem introduced with "We have a hard time balancing these aspects" in summit.git:WIP/Healing_our_community.mdwn: It was easier and more pleasurable for me to do this work while I was there, but it caused trouble for you.

Fully understood! There are (and were) absolutely no hard feelings! :)

Off-topic: I'd really like us to have coding standards, ideally not too far from established Ruby best practices. So I'll try to come back to this and do a PoC mass linting in a dedicated branch. Then we can decide how much we value personal preferences over established best practices, which may result in disabling some of the linting rules in a config file in Git, so everyone's brain/editor/IDE/linter can be aware of our coding standards.

Sounds great, fully agreed!
anonym wrote:

intrigeri wrote:

I'll look at your code review this morning and I should manage to push the corresponding follow-up commits today. Then I'll reassign to you for another review pass (without waiting for CI results).

Your fixes look good!

I'll also do another pass on the docs and tests, as I said yesterday.

I'll proceed with this now.

---

anonym wrote:

anonym wrote:

anonym wrote:

I'll also do another pass on the docs and tests, as I said yesterday.

I'll proceed with this now.

Done! Nothing new to add. :)

---

intrigeri wrote:

05/18/2020
- Status changed from Needs Validation to Resolved

Applied in changeset tails\7ca99d60e1670dc0c5daedf13a449528d5a7783.