Tails: Security, Maintainability and Usability

Pick three!

Julien Voisin Jérôme Boursier

July 4, 2016

Nuit du Hack

Who are we ?

Who are we ?

Julien Voisin

- Radare2
- NBS-System
- dustri.org

Jérôme Boursier

- AdwCleaner
- Student
- fr33tux.org

Who are we ?

Julien Voisin

- Radare2
- NBS-System
- dustri.org

Jérôme Boursier

- AdwCleaner
- Student
- fr33tux.org

nos oignons

Tails - The Amnesic Incognito Live System

Tails - The Amnesic Incognito Live System

What is Tails?

> *Tails, born in 2009, is a live operating system, aiming at preserving your privacy and anonymity.*

Tails - The Amnesic Incognito Live System

What is Tails?

Tails, born in 2009, is a live operating system, aiming at preserving your privacy and anonymity.

- All connections to the Internet are forced to go through the Tor network;
- It leaves no trace on the computer you are using unless you ask it explicitly;
- It provides cryptographic tools to encrypt your files, emails and IM.
- Secure and usable by default

Tails - The Amnesic Incognito Live System

According to the NSA

> *(S//REL) Tails: Complete Bootable OS on CD for anonymity - includes Tor*
> *(S//REL) Adds Severe CNE[1] misery to equation*

[1] Computer Network Exploitation

Tails - The Amnesic Incognito Live System

According to the NSA

> *(S//REL) Tails: Complete Bootable OS on CD for anonymity - includes Tor*
> *(S//REL) Adds Severe CNE*
>
> *These variables define terms and websites relating to the TAILs (The Amnesic Incognito Live System) software program, a comsec mechanism advocated by extremists on extremist forums.*

Tails - The Amnesic Incognito Live System

According to the NSA[1]

> *(S//REL) Tails: Complete Bootable OS on CD for anonymity - includes Tor*
> *(S//REL) Adds Severe CNE*

> *These variables define terms and websites relating to the TAILs (The Amnesic Incognito Live System) software program, a comsec mechanism advocated by extremists on extremist forums.*

[1] Thanks to a *famous* Tails user for providing these documents.

Tails - The Amnesic Incognito Live System

The life of Tails

- A major/minor release every six weeks[2]
- 2800 commits by 15+ people in the last 6 months
- The *core Tails Developers* are anonymous, mysterious and friendly.
- More than 17,000 boots per day!

[2] Synchronized with Firefox/TBB

Tails - The Amnesic Incognito Live System

Tails
theamnesicincognitolivesystem

(Yes, the logo is a smiling USB-key)

Maintainability
Usability
Security

Maintainability - Usability - Security

Maintainability

Do you remember Haven, Anonym.OS, ParanoidLinux, onionOS, Phantomix, Liberté Linux, Mempo, ..., ?

Maintainability - Usability - Security

Usability

> *If people can not use your software, they'll use something ~~shitty~~ else.*

Maintainability - Usability - Security

Security

- *Collective matters, especially for anonymity: if you don't blend in the crowd, you're a target.*

- *Your qubes-gentoo-hardened-1337 won't do much if your email recipient gets pwned.*

Maintainability

Maintainability

- The people behind Tails are a small team
- With a lot of things to get done[3].
- So, contributors are welcome, and contributions appreciated.

[1] 1338 open issues in the bugtracker

Maintainability

- The people behind Tails are a small team
- With a lot of things to get done[3].
- So, contributors are welcome, and contributions appreciated.

The less we do, the better we live

[1] 1338 open issues in the bugtracker

Relationship with upstream

Social work

- Talk to (the right) people
- Find skilled people
- Keep people interested

Relationship with upstream

Social work

- Talk to (the right) people
- Find skilled people
- Keep people interested

Technical work

- Backports, because Tails is based on Debian stable
- Upstream as much as possible
- Apparmor, libvirt, Debian, Puppet, Mumble, Tor, Thunderbird, Firefox,...

Unit test suite

Testing a liveCD is hard

- Cucumber for Behaviour Driven Development
- Sikuli for UI testing
- KVM for (nested) virtualisation
- Jenkins for running the test suite on every git push
- Blackbox testing by emulating a real user[4]
- People for manual tests

[4] this is why it takes 3 hours to run.

Puppet everywhere

Infrastructure as code

- No privileges nor internet connection needed to contribute
- Easy maintainability, (re)deployment and convergence.
- Sharing and borrowing puppet manifests

Open development

Publish everything

- Open Bugtracker
- Monthly public meetings on XMPP
- Public development channel on XMPP too
- Public Git repositories

Usability

Translations

- Tails is based on Debian, so as translated as Debian is.
- The website/documentation is available[5] in
  - English
  - French
  - Farsi
  - Italian
  - Portuguese

[5] thanks to POEdit

Installer

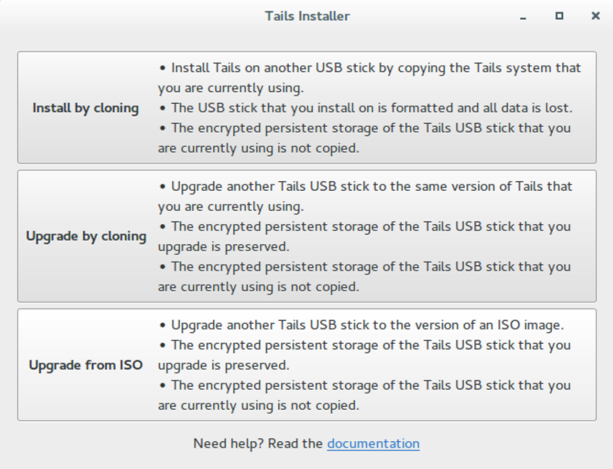
- Installing an USB key isn't straightforward
- Especially on Windows
- Especially when you need fancy encrypted partitions

Installer

- Installing an USB key isn't straightforward
- Especially on Windows
- Especially when you need fancy encrypted partitions

Hence the magical installer!

Installer (magical)



Install by cloning	• Install Tails on another USB stick by copying the Tails system that you are currently using. • The USB stick that you install on is formatted and all data is lost. • The encrypted persistent storage of the Tails USB stick that you are currently using is not copied.
Upgrade by cloning	• Upgrade another Tails USB stick to the same version of Tails that you are currently using. • The encrypted persistent storage of the Tails USB stick that you upgrade is preserved. • The encrypted persistent storage of the Tails USB stick that you are currently using is not copied.
Upgrade from ISO	• Upgrade another Tails USB stick to the version of an ISO image. • The encrypted persistent storage of the Tails USB stick that you upgrade is preserved. • The encrypted persistent storage of the Tails USB stick that you are currently using is not copied.

Need help? Read the documentation

Incremental upgrades (IUK)

- Tails is *huge* (1Gib)

Incremental upgrades (IUK)

- Tails is *huge* (1Gib)
- Not everyone has fiber-powered internet

Incremental upgrades (IUK)

- Tails is *huge* (1Gib)
- Not everyone has fiber-powered internet
- Hence incremental upgrades!

Incremental upgrades (IUK)

- Tails is *huge* (1Gib)
- Not everyone has fiber-powered internet
- Hence incremental upgrades!
- Based on:

Incremental upgrades (IUK)

- Tails is *huge* (1Gib)
- Not everyone has fiber-powered internet
- Hence incremental upgrades!
- Based on:
    - TUF - The Upgrade Framework

Incremental upgrades (IUK)

- Tails is *huge* (1Gib)
- Not everyone has fiber-powered internet
- Hence incremental upgrades!
- Based on:
    - TUF - The Upgrade Framework
    - Thandy: Automatic updates for Tor bundles

Incremental upgrades (IUK)

- Tails is *huge* (1Gib)
- Not everyone has fiber-powered internet
- Hence incremental upgrades!
- Based on:
  - TUF - The Upgrade Framework
  - Thandy: Automatic updates for Tor bundles
- Interesting threat model and challenges

Cryptography is hard

- Looking at people trying to explain *how to GPG* is fun.
- This is why we have the *OpenGPG applet*
- Automatic verification of IUK
- OTR by default in *Pidgin*

UX testing

- Give objectives to users, and watch them fail
- Identify blocking points
- Designing good UX is *awfully hard*

Documentation

- Document everything, and make this mandatory
- For users, and contributors

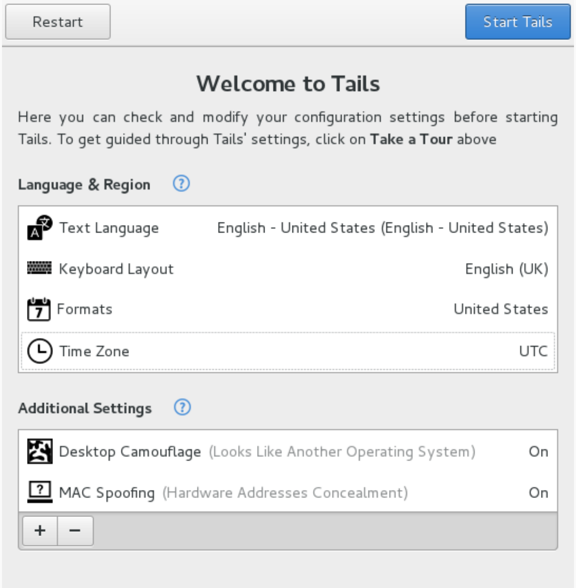
Accessibility

- Follow GNOME's *User Interface Guidelines for Supporting Accessibility*
- Use GNOME :P
- Drivers for accessibility devices
- Do one thing, and do it right
- Accessibility is super-hard

Persistence

- LUKS, dm-crypt and ext4
- UX and users are a living nightmare
- Profiles for important software/components
- Allow ~~Tails dev~~ *power-users* to persist whatever they want

Greeter



Welcome to Tails

Here you can check and modify your configuration settings before starting Tails. To get guided through Tails' settings, click on **Take a Tour** above

Language & Region ?

Text Language	English - United States (English - United States)
Keyboard Layout	English (UK)
Formats	United States
Time Zone	UTC

Additional Settings ?

Desktop Camouflage (Looks Like Another Operating System)	On
MAC Spoofing (Hardware Addresses Concealment)	On

Support

(Un)fortunately, Tails has users

- Whisperback to report bugs

Support

(Un)fortunately, Tails has users

- Whisperback to report bugs
- Frontdesk to answer emails

Support

(Un)fortunately, Tails has users

- Whisperback to report bugs
- Frontdesk to answer emails
- Mailing lists

Support

(Un)fortunately, Tails has users

- Whisperback to report bugs
- Frontdesk to answer emails
- Mailing lists
- IRC / XMPP

Support

Speaking of users...

Support

(Un)fortunately, Tails has users that play

> *< lskitto> Just a suggestion but in the next update can you include Minecraft?*

Support

(Un)fortunately, Tails has users that know better (cont.)

22:41 eborberma> there may be fewer security issues if tails used more python software
22:42 ghetto> or less java software
22:43 eborberma> there is no java in tails

Support

(Un)fortunately, Tails has users that know better

> *< Shikila> There are many papers, don't act so blind*
> *< BitingBird> ...*
> *< Shikila> If I actualy studied computers I myself would have proably wrote one*

Support

(Un)fortunately, Tails has users that want flash

< t4nk860> hello have a question

< t4nk860> how do i install flash player in tails

Support

(Un)fortunately, Tails has users that are looking for fancy things

> *02:28 xecuter > how i find the secret communications of us military forces in the deep web?*

Support

(Un)fortunately, Tails has users that, err, well...

> *23:07 PETE255 > hi you assholes HOW THE FUCK DO YOU INSTALL AN UNOFFICIAL DEBIAN FUCKING PAGKAGE DICKHEADS*

Support

(Un)fortunately, Tails has users that are *creative*

> *< ghetx> can i use a _ for password?*

Support

(Un)fortunately, Tails has users that are candid

> *< klapaucius> is there a good tor website for saving passwords?*

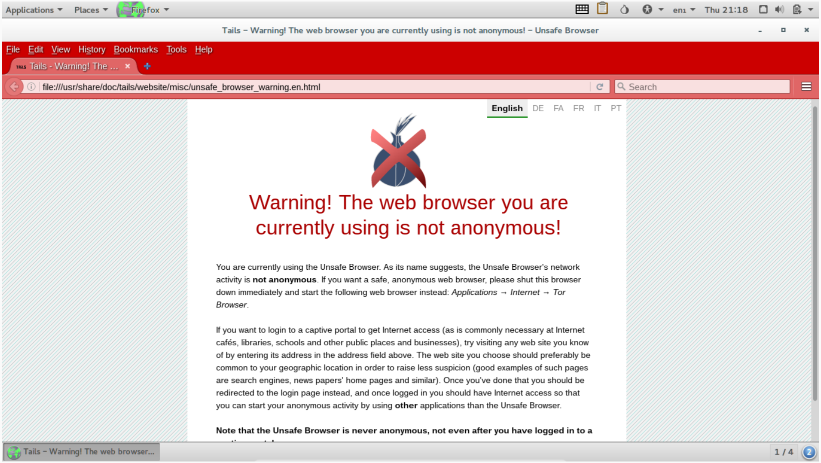
Support

Fortunately, we have ~~popcorn~~ patience!

Unsafe browser

- Captive portals are annoying
- Use the unsafe browser to access them
- Use a scary red theme for it
- But people will use it for anything else anyway.

Scary unsafe browser



Applications
Places
Firefox
en₁
Thu 21:18
Tails – Warning! The web browser you are currently using is not anonymous! – Unsafe Browser
File
Edit
View
History
Bookmarks
Tools
Help
Tails - Warning! The ...
file:///usr/share/doc/tails/website/misc/unsafe_browser_warning.en.html
Search
English
DE
FA
FR
IT
PT
Tails – Warning! The web browser...
1 / 4

Warning! The web browser you are currently using is not anonymous!

You are currently using the Unsafe Browser. As its name suggests, the Unsafe Browser's network activity is **not anonymous**. If you want a safe, anonymous web browser, please shut this browser down immediately and start the following web browser instead: *Applications → Internet → Tor Browser*.

If you want to login to a captive portal to get Internet access (as is commonly necessary at Internet cafés, libraries, schools and other public places and businesses), try visiting any web site you know of by entering its address in the address field above. The web site you choose should preferably be common to your geographic location in order to raise less suspicion (good examples of such pages are search engines, news papers' home pages and similar). Once you've done that you should be redirected to the login page instead, and once logged in you should have Internet access so that you can start your anonymous activity by using **other** applications than the Unsafe Browser.

Note that the Unsafe Browser is never anonymous, not even after you have logged in to a

Binary blobs

Binary blobs are a truly amazing trolling source!

Binary blobs

Binary blobs are a truly amazing trolling source!

But remember the previously mentioned mantra:

Binary blobs

Binary blobs are a truly amazing trolling source!

But remember the previously mentioned mantra:

> *If people can not use your software, they'll use something ~~shitty~~ else.*

Security

Threat model

Attackers are:

- Global
- Powerful
- Smart

Threat model

Attackers are:

- Global
- Powerful
- Smart

Users are:

- Global
- Powerless
- Well...

Persistence (cont.)

Persistence can improve security

- Persisting the *PRNG* state
- Persisting Tor cache for a quicker startup
- Persisting bridges is on the todo-list, but it's non-trivial.

Emergency releases

Because people like to drop public exploits[6].

- Synchronisation with upstream
- Emergency releases are done in less than 24h.
- Those aren't fun to do.

[6] And not only shitty XSS.

Signature verification

Did anyone ever told you that gpg is hard?

- Releases are signed[7]
- But no one knows how to use *gpg*.
- Browser addon to download and verify.

[7] Key management is fun!

Reproducible builds

We have trust issues.

- Reproducible builds for software may be non-trivial
- Reproducible builds for ISO are non-trivial
- Also, sustainability: we don’t have to trust the *release manager*.

Apparmor

Easy sandboxing as much as possible

- No one knows how to write SELinux rules
- Is anyone using Tomoyo?
- Every internet-facing service has an Apparmor profile
- *Interesting* binaries[8] too.
- Almost everything is pushed upstream

[8] Like the one parsing PDF.

What about grsecurity ?

> “Every time someone mentions *grsecurity* and *tails* in the same sentence, take a drink.”
>
> — An anonymous Tails contributor

What about grsecurity ?

More seriously

- No grsecurity package in Debian.

What about grsecurity ?

More seriously

- No grsecurity package in Debian.
- The Tails dev are not kernel developers.

What about grsecurity ?

More seriously

- No grsecurity package in Debian.
- The Tails dev are not kernel developers.
- Corsac is now maintaining one.

What about grsecurity ?

More seriously

- No grsecurity package in Debian.
- The Tails dev are not kernel developers.
- Corsac is now maintaining one.
- Tails uses aufs for persistence

What about grsecurity ?

More seriously

- No grsecurity package in Debian.
- The Tails dev are not kernel developers.
- Corsac is now maintaining one.
- Tails uses aufs for persistence
- Grsecurity doesn't like aufs.

What about grsecurity ?

More seriously

- No grsecurity package in Debian.
- The Tails dev are not kernel developers.
- Corsac is now maintaining one.
- Tails uses aufs for persistence
- Grsecurity doesn't like aufs.
- Tails is moving to overlayfs anyway.

What about grsecurity ?

More seriously

- No grsecurity package in Debian.
- The Tails dev are not kernel developers.
- Corsac is now maintaining one.
- Tails uses aufs for persistence
- Grsecurity doesn't like aufs.
- Tails is moving to overlayfs anyway.
- AppArmor doesn't like overlayfs.

What about grsecurity ?

More seriously

- No grsecurity package in Debian.
- The Tails dev are not kernel developers.
- Corsac is now maintaining one.
- Tails uses aufs for persistence
- Grsecurity doesn't like aufs.
- Tails is moving to overlayfs anyway.
- AppArmor doesn't like overlayfs.
- Nor does tails-iuk, or live-boot.

What about grsecurity ?

More seriously

- No grsecurity package in Debian.
- The Tails dev are not kernel developers.
- Corsac is now maintaining one.
- Tails uses aufs for persistence
- Grsecurity doesn't like aufs.
- Tails is moving to overlayfs anyway.
- AppArmor doesn't like overlayfs.
- Nor does tails-iuk, or live-boot.
- Improve grsecurity compatibility with aufs?

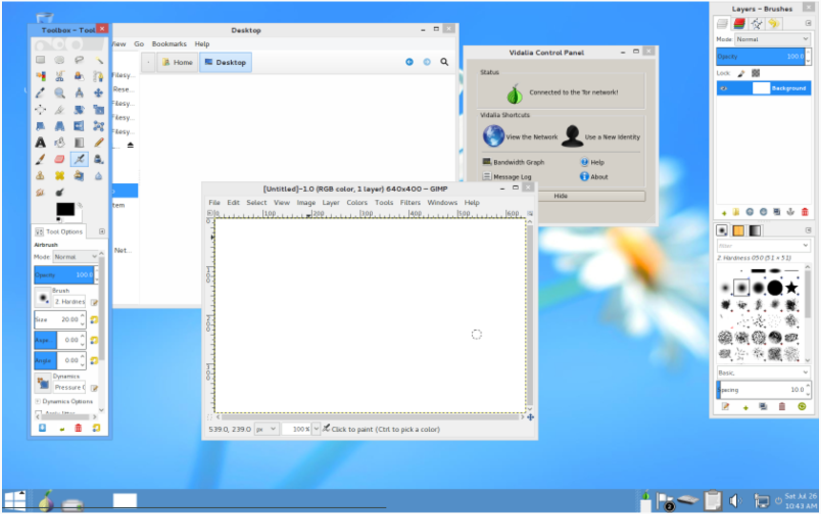
What about grsecurity ?

More seriously

- No grsecurity package in Debian.
- The Tails dev are not kernel developers.
- Corsac is now maintaining one.
- Tails uses aufs for persistence
- Grsecurity doesn't like aufs.
- Tails is moving to overlayfs anyway.
- AppArmor doesn't like overlayfs.
- Nor does tails-iuk, or live-boot.
- Improve grsecurity compatibility with aufs?
- ...

Camouflage!

Everyone is using Windows, so...[9]



Connected to the Tor network!

[Untitled]-1.0 (RGB color, 1 layer) 640x400 – GIMP

539.0, 239.0 px 100% Click to paint (Ctrl to pick a color)

[9] Unfortunately, it's not available anymore :/

Some fancy tools

Some cool Tails-born goodies:

- Memory Erasure as an anti-forensic measure

Some fancy tools

Some cool Tails-born goodies:

- Memory Erasure as an anti-forensic measure
- Shutdown on key removal

Some fancy tools

Some cool Tails-born goodies:

- Memory Erasure as an anti-forensic measure
- Shutdown on key removal
- Metadata Anonymisation Toolkit

Some fancy tools

Some cool Tails-born goodies:

- Memory Erasure as an anti-forensic measure
- Shutdown on key removal
- Metadata Anonymisation Toolkit
- Mac spoofing

Some fancy tools

Some cool Tails-born goodies:

- Memory Erasure as an anti-forensic measure
- Shutdown on key removal
- Metadata Anonymisation Toolkit
- Mac spoofing
- Network disabling

Some fancy tools

Some cool Tails-born goodies:

- Memory Erasure as an anti-forensic measure
- Shutdown on key removal
- Metadata Anonymisation Toolkit
- Mac spoofing
- Network disabling
- ...

Conclusion

Conclusion

- Everyone can use Tails

Conclusion

- Everyone can use Tails
- Seven years old, still alive!

Conclusion

- Everyone can use Tails
- Seven years old, still alive!
- Anonymity and amnesia as security features

Conclusion

- Everyone can use Tails
- Seven years old, still alive!
- Anonymity and amnesia as security features
- Security and Maintainability and Usability

Thank you!

Tails

the**amnesic**incognito**live**system

Questions?

Protip 1: If your question has more than 3 parts, it's wrongly phrased.

Protip 2: If your sentence doesn't end with a ? it's not a question.