



# Tails

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



# Tails

the amnesic incognito live system

## Agenda

- Was ist Tails?
- Wie funktioniert Tails?
- Welche Verbindungsmethode nutzt Tails?
- Welche Sicherheitslücken sind aufgetreten?
- Welche Risiken bezüglich Überwachung/Malware bestehen?
- News rund um Tails
- Funktionen in Tails
- Praktische Vorführung des Systems
- Diskussionsfrage



# Tails

the amnesic incognito live system

## Was ist Tails?

- The **amnesic incognito live system**

**Amne|sie** (*die; -, Nomen*)

[gr.-nlat.: *a* „ohne, nicht“, *mnesis* „Erinnerung“]

Form des Gedächtnisschwunds; bspw.: Verlust des Langzeitgedächtnisses.

**in|ko|gni|to** (*Adverb / das; -, Nomen*)

[lat.-it.: *in-* (verneinend), *cognoscere* „erkennen; bemerken“]

Einer Person: unter fremdem Namen auftretend; unidentifizierbar.

## Wofür wurde es entwickelt?

- Life-Betriebssystem über Stick/DVD/SD-Karte
- Ziel: Privatsphäre und Anonymität durch:
  - Anonym surfen, Zensur umgehen
  - Keine Spuren auf PC
  - Aktuellste kryptographische Werkzeuge zur Datei- / Mail- / Messaging-Verschlüsselung



# Tails

the amnesic incognito livesystem

## Wer nutzt Tails?

- „normale“ User
- „Maulwürfe“ und Spione
- Kriminelle
- Whistleblower (Edward Snowden)
  - Mittlerweile empfohlen: Qubes OS (8.11.2016)





# Tails

the amnesic incognito live system

## Wer steckt hinter Tails?

- Lediglich Nicknames zu finden
- intrigeri, jvoisin, u, sajolida, BitingBird, alan...
- 
- Kontakt über Mailing-Listen (themenbezogen)
  - amnesia-news
  - Tails-project
  - Tails-dev
  - Tails-testers
  - Tails-ux
  - ...

### tails-project

tails-project@boum.org is the mailing list where we discuss upcoming events, monthly reports, and other non-technical matters.

Public archive of tails-project: <https://mailman.boum.org/pipermail/tails-project/> ↗.

Subscribe



# Tails

the amnesic incognito live system

## Wie funktioniert Tails?

- Open Source Software
- Debian GNU/Linux-basiert
- GNOME-Desktop
- Keine Festplattennutzung
- Nur RAM => automatische Löschung bei Herunterfahren
- => Keinerlei Spuren
- Kryptographische Werkzeuge auf aktuellem Stand



# Tails

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

Welche Verbindungsmethode nutzt Tails?

- Jede Internetverbindung über Tor
- 
- Optional: Tor-Bridgemode
- 
- Alle anderen Internetverbindungen geblockt
- 
- Verschleiern der MAC-Adresse



# Tails

the amnesic incognito livesystem

## Welche Sicherheitslücken sind aufgetreten?

Mehrere Sicherheitslücken in Tails 2.10 wurden in Tails 2.11 geschlossen.

Wir empfehlen **dringend** so bald wie möglich eine Aktualisierung auf [Tails 2.11](#) durchzuführen.

- Tor Browser: [Mozilla Foundation Security Advisory 2017-06](#) - linux-image-4.8.0-0.bpo.2-686-unsigned: [2017-6074](#) - bind9: [Debian Security Advisory 3795](#) - imagemagick: [Debian Security Advisory 3799](#) - libevent-2.0-5: [Debian Security Advisory 3789](#) - libgd3: [Debian Security Advisory 3777](#) - libjasper1: [Debian Security Advisory 3785](#) - liblcms2-2: [Debian Security Advisory 3774](#) - libxpm4: [Debian Security Advisory 3772](#) - login: [Debian Security Advisory 3793](#) - ntfs-3g: [Debian Security Advisory 3780](#) - openjdk-7-jre: [Debian Security Advisory 3782](#) - openssl: [Debian Security Advisory 3773](#) - tcpdump: [Debian Security Advisory 3775](#) - vim: [Debian Security Advisory 3786](#) - libreoffice: [Debian Security Advisory 3792](#)

Installieren Sie  
**Tails 2.12**

2017-04-19



Über Tails

Erste Schritte...

Dokumentation

Hilfe & Support

Mitmachen

Aktuelles



Spenden





# Tails

the amnesic incognito live system

## Debian Security Advisory

### DSA-3827-1 jasper -- security update

**Date Reported:**

07 Apr 2017

**Affected Packages:**

[jasper](#)

**Vulnerable:**

Yes

**Security database references:**

In Mitre's CVE dictionary: [CVE-2016-9591](#), [CVE-2016-10249](#), [CVE-2016-10251](#).

**More information:**

Multiple vulnerabilities have been discovered in the JasPer library for processing JPEG-2000 images, which may result in denial of service or the execution of arbitrary code if a malformed image is processed.

For the stable distribution (jessie), these problems have been fixed in version 1.900.1-debian1-2.4+deb8u3.



# Tails

the amnesic incognito livesystem

Welche Risiken bezüglich Überwachung/Malware bestehen?

- Kompromittierte Hardware (Bios, Firmware)
- Tail-Installation von kompromittiertem System
- Tor-Ausgangsrelais
- Sichtbar, dass Tails/Tor genutzt wird
- Man-in-the-Middle-Angriffe
- Bestätigungsangriffe (Zusammenpassen des Ein- und Ausgangstraffics)



# Tails

the amnesic incognito live system

Welche Risiken bezüglich Überwachung/Malware bestehen?

- Dokumente nicht standardmäßig verschlüsselt
- Metadaten einiger Dateiformate
- Unverschlüsselte Header
- Schlechte Passwörter
- Kontinuierliche Weiterentwicklung wirkt dagegen



# Tails

the amnesic incognito livesystem

Welche Risiken bezüglich Überwachung/Malware bestehen?

- Möglicher Vertrauensabzug: Finanzierung
  - 210 T€ / Jahr im Durchschnitt
  - 1/3 der Spender Bezug zur US-Regierung
  - 1/3 Stiftungen und NGOs
  - 1/3 Einzelpersonen (17%) und Unternehmen (15%)
- Kaltstartattacken
- Tails überschreibt RAM beim Ausschalten



# Tails

the amnesic incognito livesystem

## News rund um Tails

- <https://tails.boum.org/news/index.de.html>
- Aufruf für Beta-Tester Version 3.0~beta4
  - Debian 9
  - Security Fixes
  - Allgemeine Bug-Fixes
- 17.03.16 „Tails – das Betriebssystem für gemäßigt Paranoide“ - Zeit.de
- 
- 27.01.16 „Tails 2.0: Das Anonymisierungs-OS im neuen Look“ - heise.de



# Tails

the amnesic incognito live system

## Installation von Tails

- Download und Verifizierung über Plugin
- Installationsanleitung auf [tails.boum.org](https://tails.boum.org)
- Bootfähigen Stick erstellen
- Temporäres Tails installieren (Windows)
- Temporäres Tails starten
- Finales Tails installieren

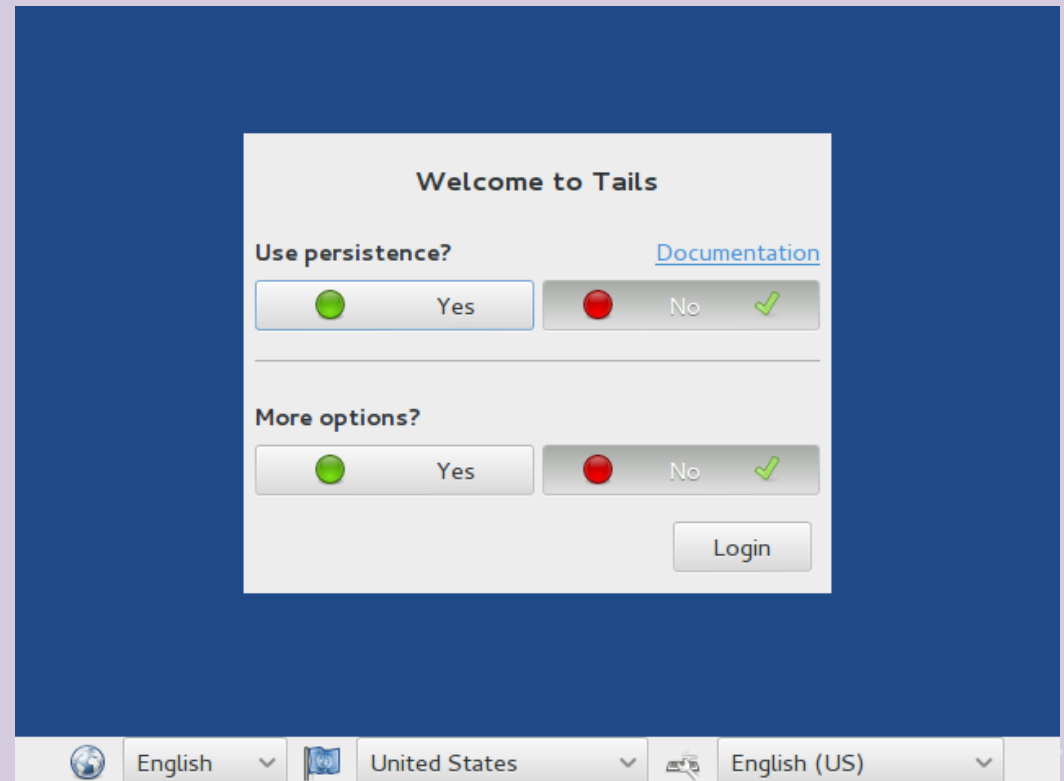


# Tails

the amnesic incognito livesystem

## Funktionen in Tails

- 
- Startmodi: Normal; Troubleshooting
- Tails Greeter
  - Adminpasswort
  - MAC verschleiern
  - Netzwerk
    - Tor-Bridge
    - Offline-Modus
  - Persistenter Speicher





# Tails

the amnesic incognito live system

## Funktionen in Tails

Kryptographische Werkzeuge auf aktuellem Stand

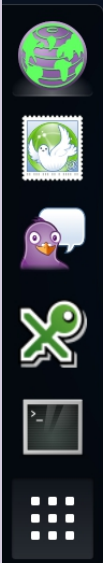
- LUKS
- HTTPS Everywhere
- OpenPGP
- OTR
- Nautilus Wipe





# Tails

the amnesic incognito livesystem



About Tails



Archive Manager



Audacity



bookletimposer



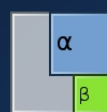
Brasero



Calculator



Configure persistence...



Dasher



Delete persistent ...



Disks



Document Viewer



Electrum Bitcoin ...



Files



Florence Virtual K...



gedit



GNU Image Manipu...



Gobby



GtkHash



Help



Icedove



Image Viewer



Inkscape



KeePassX



Libre Office



# Tails

the amnesic incognito live system

## Funktionen in Tails

- Messenger
- Internetbrowser
- Mail-Client
- Audio/Videoschnitt
- Office
- Zubehör
- Systemanwendungen
- weitere Programme installieren



# Tails

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

## **Praktische Vorführung des Systems**



# Tails

the amnesic incognito livesystem

## Diskussionsfragen

- Wie schätzt ihr die Nutzbarkeit von Tails für den alltäglichen Gebrauch ein?
- 
- Kompromiss: Funktionenvielfalt vs Anonymität?
- 
- Missbrauchsmöglichkeiten durch Anonymität?



# Tails

the amnesic incognito livesystem

## Quellen:

Autor der Präsentation: Felix Kulle

## Bildquellen:

Folie 1, Hintergrund: <https://tails.boum.org/index.de.html>

Folie (Wer nutzt Tails)

<http://www.googlewatchblog.de/wp-content/uploads/Edward-Snowden.jpg>

Folie (Wer steckt hinter...)

<https://tails.boum.org/about/contact/index.en.html>

## Literaturquellen:

Wer nutzt Tails

<https://tarnkappe.info/edward-snowden-setzt-nicht-mehr-auf-tails-qubes-os-vorgestellt/>

Folie (Was ist Tails?)

<https://tails.boum.org/about/index.de.html>

Folie (Wer steckt hinter...)

<https://tails.boum.org/about/contact/index.en.html>

<https://tails.boum.org/contribute/index.en.html>



# Tails

the amnesic incognito live system

Quellen:

Bildquellen:

Sicherheitslücken:

[https://tails.boum.org/security/Numerous\\_security\\_holes\\_in\\_2.11/index.de.html](https://tails.boum.org/security/Numerous_security_holes_in_2.11/index.de.html)

<https://www.debian.org/security/2017/dsa-3827>

Literaturquellen:

Funktionen/Wie funktioniert Tails

<https://tails.boum.org/about/index.de.html>

[https://tails.boum.org/doc/first\\_steps/startup\\_options/index.de.html](https://tails.boum.org/doc/first_steps/startup_options/index.de.html)

Risiken

<https://tails.boum.org/doc/about/warning/index.de.html>

[https://tails.boum.org/news/why\\_we\\_need\\_donations/index.de.html](https://tails.boum.org/news/why_we_need_donations/index.de.html)