

Tails

System do anonimowego surfowania po sieci

Kamil Woźniak

Wydział Fizyki, Matematyki i Informatyki
Politechnika Krakowska

10.11.2015

Przegląd

- 1 Pierwsze kroki
 - Instalacja
 - Konfiguracja

- 2 Użytkowanie

Tails

Wprowadzenie

- The Amnesic Incognito Live System (TAILS) – dystrybucja Linuxa oparta na Debianie, mająca na celu zachować prywatność i anonimowość (tzw. incognito) podczas korzystania z internetu. Jest kontynuacją projektu Incognito LiveCD.
- TAILS można używać na dowolnym komputerze, nie zostawiając przy tym żadnych śladów (chyba, że użytkownik zażyczy sobie inaczej).

Tails

Wprowadzenie

- Jest to kompletny system operacyjny przeznaczony do działania z zewnętrznego nośnika takiego jak płyta DVD, pamięć USB czy karta pamięci SD. Działa przy tym niezależnie od zainstalowanego macierzystego systemu operacyjnego.
- TAILS udostępniany jest na darmowej licencji opartej na Debian GNU/Linux. System posiada zainstalowanych kilka pre-konfigurowanych aplikacji mających pomóc w anonimowym i bezpiecznym korzystaniu z zasobów internetowych.

Tails

Wprowadzenie

- TAILS opiera się na sieci Tor (ang. The Onion Router) i uniemożliwia użytkownikowi bezpośredni dostęp do sieci, dzięki czemu pozwala zachować niemal całkowitą anonimowość, ukrywa naszą lokalizację i daje dostęp do różnych ocenianych serwerów.
- TAILS może również korzystać z sieci i2p (ang. Invisible Internet Project), również mającej na celu zwiększenie anonimowości i bezpieczeństwa w sieci.
- Dzięki korzystaniu tylko z pamięci RAM, użytkownicy systemu nie są narażeni na pozostawienie po sobie informacji na dysku twardym danego komputera.
- System TAILS posiada również szereg narzędzi służących do szyfrowania informacji oraz trwałego usuwania danych.

Tails

Wymagania systemowe

- Czytnik płyt DVD lub możliwość rozruchu systemu z pamięci USB lub karty SD.
- Procesor kompatybilny z x86.
- 2GB pamięci RAM to płynnej pracy.

Tails

Instalacja

- Chcąc korzystać z systemu TAILS użytkownik zwykle staje przed wyborem między nośnikiem DVD a pamięcią USB bądź kartą SD.
- Nośnik DVD jest znacznie tańszy, ale nie pozwala na aktualizację do nowych wersji, więc za każdym razem chcąc korzystać z nowszej wersji systemu trzeba wypalać nową płytę. Rozwiązaniem może być jednak nośnik DVD-RW pozwalający nadpisywać istniejące dane.
- Drugi wariant może być problematyczny na niektórych starszych urządzeniach nie obsługujących rozruchu z USB czy slotu kart pamięci.

Tails

Tworzenie nośnika DVD-R z systemem TAILS.

W celu utworzenia nośnika DVD-R z systemem TAILS należy wypalić obraz systemu przy użyciu wybranego programu do tego służącego.

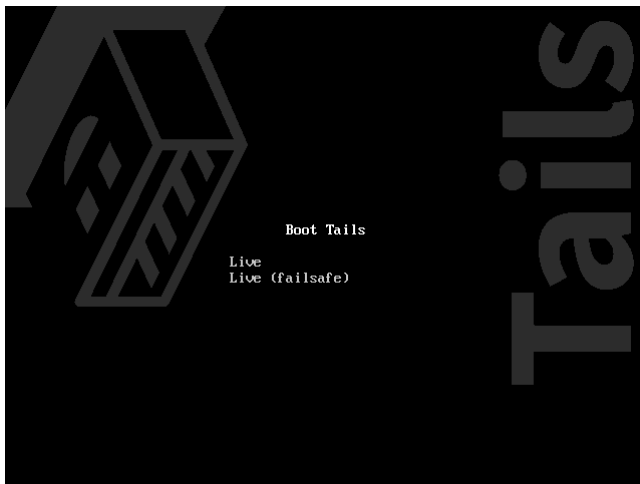
Tails

Uruchamianie

- By uruchomić system TAILS z płyty DVD wystarczy umieścić nośnik w odpowiednim napędzie DVD i zrestartować komputer.
- Po ponownym uruchomieniu naszym oczom powinno się ukazać menu startowe

Tails

Uruchamianie



Tails

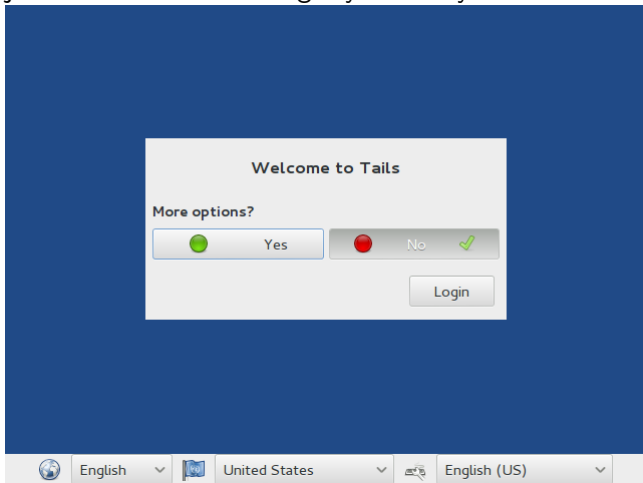
Uruchamianie

- Opcja druga (failsafe) wyłącza niektóre cechy jądra, dzięki czemu może działać lepiej na komputerach, na których występują błędy, które podejrzewamy, że są wywołane przez brak kompatybilności systemu z naszym sprzętem.
- Można dodać dodatkowe opcje za pomocą klawisza Tab. Na dole ekranu pojawiają się wtedy wtedy wszystkie dodatkowe opcje.
- By dodać konkretną opcję należy nacisnąć klawisz Spacja i wpisać nazwę pożądaney opcji (można dodać kilka naraz oddzielając nazwy Spacją).
- Następnie wystarczy nacisnąć Enter by uruchomić system.

Tails

Uruchamianie

Między menu startowym a pulpitem GNOME pojawia się jeszcze zbiór okien dialogowych zwanych Tails Greeter.



Tails

Konfiguracja

- Wybór języka polskiego.

W celu wybrania innego języka należy skorzystać z menu u dołu ekranu i zmienić ustawienie z English na odpowiednią inną nazwę. Mamy również możliwość ustawieniu więcej opcji, gdzie można zarządzać hasłami, konfiguracją sieci czy szyfrowaniem. Aby uruchomić TAILS klikamy na przycisku login.

Tails

Dodatkowe oprogramowanie

- Aby zainstalować dodatkowe oprogramowanie lub uzyskać dostęp do wewnętrznego dysku twardego, musimy mieć przywileje Administratora. Domyślnie hasło administratora jest wyłączone.
- W celu ustawienia hasła administratora należy na ekranie startowym wybierać Yes, po czym kliknąć przycisk w przód, po czym ustawić hasło w sekcji Hasło administracyjne.

Tails

Korzystanie z terminala

- Terminal można uruchomić wybierając Aplikacje, następnie Akcesoria i dalej Terminal.

Tails

Windows camouflage

- Podczas użytkowania systemu w miejscu publicznym można skorzystać z opcji Kamuflaż systemu Windows. Aby skorzystać z opcji należy na ekranie Tails Greeter wybrać Tak, po czym kliknąć na przycisku w przód i w sekcji 2. Kamuflaż systemu Windows wybrać Aktywuj Kamuflaż Microsoft Windows 8.

Tails

Windows camouflage



Tails

Spoofing adresu MAC

- System TAILS pozwala na ukrycie numeru seryjnego karty sieciowej przed lokalnymi sieciami, co może pomóc ukryć położenie geograficzne użytkownika. Może to jednak wzbudzić podejrzenia lub przysparzać problemy z połączeniem.
- Domyślnie opcja ta jest włączana. Aby wyłączyć należy wybrać Tak w Tails Greeter i kliknąć na przycisku w przód. Następnie trzeba odznaczyć opcję Spoof'uj wszystkie adresy MAC.

Tails

Konfiguracja połączenia

- W zależności od posiadanego połączenia, może nastąpić konieczność konfiguracji sposobu, w jaki Tor łączy się z Internetem.
- Aby zmienić ustawienia, w Tails Greeter wybieramy Tak, a następnie klikamy na przycisku w przód. Następnie w sekcji Konfiguracja sieci wybieramy opcję Połączenie internetowe tego komputera jest ocenzone, filtrowane lub przepuszczane przez proxy. Można również skonfigurować most, firewall lub ustawienia proxy.
- Po wykonaniu powyższych czynności i po uruchomieniu sesji roboczej, asystent poprowadzi nas przez konfigurację sieci Tor. Można również wybrać opcję Disable all networking w celu pracy offline.

Tails

Mosty Tor

- Chcąc z jakichś powodów ukryć fakt, że korzysta się z sieci Tor można skorzystać z tzw. mostów Tor(ang. Tor bridges), które są alternatywnymi wejściami do sieci Tor, niebędącymi udostępnionymi publicznie.
- Aby włączyć, wybieramy Tak w Tails Greeter, a następnie przycisk w przód. Dalej, w sekcji Konfiguracja sieci wybieramy opcję Połączenie internetowe tego komputera jest odcenzurowane, filtrowane lub przepuszczane przez proxy. Możesz skonfigurować most, firewall lub ustawienia proxy.
- Następnie, po uruchomieniu sesji roboczej, asystent poprowadzi nas przez konfigurację sieci Tor, gdzie możemy również skonfigurować Tor bridge. Wadą mostów jest ich wydajność.

Tails

Korzystanie z trwałej objętości dyskowej

- Przy uruchamianiu systemu TAILS z pamięci USB lub karty SD jest możliwość utworzenia trwałej objętości dyskowej z przestrzeni dyskowej niezajętej przez system, gdzie wszystkie pliki są szyfrowane przed zapisem i można uzyskać do nich dostęp w oddzielnych sesjach.

Tails

Instalacja dodatkowych aplikacji

- TAILS jest wyposażony w limitowaną liczbę zainstalowanych aplikacji, które jednak są dokładnie przetestowane pod kątem bezpieczeństwa w sieci.
- Można instalować aplikacji kompatybilne z Debianem.
- Każda nowo zainstalowana aplikacja, która łączy się z Internetem musi najpierw zostać poprawnie skonfigurowana w celu korzystania z sieci Tor.
- Ponadto aplikacje trzeba instalować za każdym razem rozpoczynając nową sesję. Można również skorzystać z funkcji automatycznej instalacji przy każdym starcie systemu.

Tails

Instalacja dodatkowych aplikacji

- TAILS jest wyposażony w limitowaną liczbę zainstalowanych aplikacji, które jednak są dokładnie przetestowane pod kątem bezpieczeństwa w sieci.
- Aby zainstalować dodatkowe pakiety ustawiamy hasło administratora. Następnie otwieramy terminal i wykonujemy komendę „apt-get update” w celu aktualizacji listy dostępnych pakietów. By zainstalować pakiet wykonujemy komendę „apt-get install [pakiet]” gdzie w miejsce „[pakiet]” wpisujemy nazwę pożądanego pakietu, np. „apt-get install abc”, by zainstalować pakiet abc.
- Można także instalować kilka pakietów naraz.

Tails

Wyłączanie systemu TAILS

System Tails można wyłączyć na kilka sposobów:

- 1. Klikając na ikonie wyłączenia systemu w górnym-prawym rogu ekranu a następnie wybierając opcję Wyłącz natychmiast lub Zresetuj natychmiast.
- 2. Naciskając przycisk zasilania komputera.
- 3. rzez fizyczne usunięcie nośnika, z którego uruchomiony jest TAILS.

Podczas wyłączenia, pamięć RAM jest wymazywana w celu ochrony przed tzw. cold boot attacks.

Dziękuję za uwagę!