Written by **C. Mitchell Shaw** on October 1, 2017

Tails 3.2: Privacy, Security, and Anonymity on the Internet Just Got Easier

The operating system Ed Snowden used to communicate with journalists when he revealed the size and scope of NSA surveillance in 2013 received a major update Thursday. Tails (which stands for The Amnesic Incognito Live System) is a Linux distribution created and distributed by the Tails Project. Tails is built from the ground up to offer security, privacy, and anonymity to computer users everywhere.

Tails — which is described by its developers as "privacy for anyone anywhere" — has been around since 2009 and has received the Mozilla Open Source Support Award (2016), the Access Innovation Prize (2014), and the OpenITP award (2013). More importantly, it has been used by dissidents in oppressive nations, activists who feel the need to remain anonymous, whistleblowers, and investigative journalists. In fact, the three journalists most involved in the Snowden revelations all used Tails when communicating with him about NSA surveillance. Snowden insisted on it. In April 2014, Freedom of the Press Foundation reported that Laura Poitras, Glenn Greenwald, and Barton Gellman all told the foundation that Tails was instrumental in allowing them to communicate with Snowden about NSA surveillance while avoiding the very surveillance they were preparing to report on.

Poitras said:

> I've been reluctant to go into details about the different steps I took to communicate securely with Snowden to avoid those methods being targeted. Now that Tails gives a green light, I can say it has been an essential tool for reporting the NSA story. It is an all-in-one secure digital communication system (GPG email, OTR chat, Tor web browser, encrypted storage) that is small enough to swallow. I'm very thankful to the Tails developers for building this tool.

Greenwald agreed, saying that Tails was "vital to my ability to work securely on the NSA story," adding, "The more I've come to learn about communications security, the more central Tails has become to my approach."

And Gellman, recognizing that while "privacy and encryption work," it can be "easy to make a mistake that exposes you." He said that "Tails puts the essential tools in one place, with a design that makes it hard to screw them up." He added, "I could not have talked to Edward Snowden without this kind of protection. I wish I'd had it years ago."

Tails is a full Linux distribution that runs from a USB stick or DVD. It can be loaded on almost any computer and — because it runs from the USB stick or DVD using the computer's memory instead of being installed on the hard drive — it leaves no trace of having been used. And because it runs from a USB stick or DVD and it can run from almost any modern computer, Tails is portable. A user can carry a Tails USB stick with him everywhere he goes and use it almost anywhere.

The description of Tails on the website where it is available as a free download says:

> Tails is a live system that aims to preserve your privacy and anonymity. It helps you to use the Internet anonymously and circumvent censorship almost anywhere you go and on any computer but leaving no trace unless you ask it to explicitly.
>
> It is a complete operating system designed to be used from a USB stick or a DVD independently of the computer's original operating system. It is Free Software and based on Debian GNU/Linux.
>
> Tails comes with several built-in applications pre-configured with security in mind: web browser, instant messaging client, email client, office suite, image and sound editor, etc.

The Web browser built into Tails is the Tor browser. Tor (which originally stood for The Onion Router) uses layers of encryption and IP spoofing to hide the location and identity of its users. Rather than connecting directly to the Internet, Tor encrypts the traffic, creates a fake IP address, and forwards the traffic to a Tor "node." That node decrypts the traffic, assigns a new fake IP address, re-encrypts the traffic and sends it to another Tor node. That process is repeated multiple times before an "exit node" delivers the traffic to the Internet and sends it on to its final destination.

Unless the user does something to identify himself (such as logging into an account associated with his real identity), no one — not the owner of the website he visits, not the NSA, no one — can know his real location or identity.

The biggest difference between just running Tor — which is a modified version of the Mozilla Firefox browser — and running Tails is that in Tails, all traffic is forced to go through the Tor network. Besides that, as Poitras pointed out, Tails comes loaded with other tools that lend themselves to privacy, security, and anonymity. All of that adds up to a Linux distribution that the NSA hates with a passion.

In fact, as part of a December 2014 article on the NSA's surveillance program, *Der Spiegel* published slides that were part of an NSA internal presentation in June 2012. The slides — part of the Snowden leaks — said that Tails (when used all by itself) is a "major threat" to the NSA's surveillance program and that when used in conjunction with other tools such as OTR (Off The Record, a secure, anonymous, encrypted messaging service that is included in Tails), the result is "catastrophic" and leads to a "near-total loss/lack of insight to target communications."

The NSA hates Tails so much, that a note in the programming for Xkeyscore (one of the NSA's most invasive surveillance tools) refers to Tails as "a comsec [communications security] mechanism advocated by extremists on extremist forums." And in July 2014, it was reported that Xkeyscore was used to identify people who visit the Tails website or even search the web for Tails. In fact, the NSA went so far as to identify *Linux Journal* (a magazine for users of the Linux operating system, which includes Wall Street IT personnel, crewmen aboard Navy submarines, personnel at the Department of Defense, personnel at the Federal Aviation Industry, and personnel at the U.S. post office, as well as too many others to list here) as an "extremist forum" whose readers are deserving of being monitored.

The Catch 22 is that going to the Tails website to download Tails to prevent being monitored gets onself identified as an "extremist" who "needs" to be monitored. However, there are ways to download Tails without the NSA or anyone else being aware of it.

Tails is well known in computer security circles as a stable, reliable operating system that does what it says. This newest update to Tails 3.2 includes several security updates. This is critical, since security is a moving target. This update also adds some new functionality and improvements in the User Interface.

Changes include:

- More ways to connect to the Internet (including dial-up connections)
- BookletImposer (to convert linear PDF documents into booklets and vice-versa)
- A new virtual keyboard (to help users get around the possibility of key-loggers)
- An upgrade to the 4.12.12 Linux kernel (to improve hardware support for more devices)
- A newer version of the Thunderbird e-mail program (similar in functionality to Outlook)
- An easier way to upgrade a Tails USB stick when new versions are released

The User Interface is simple, clean, and intuitive. Using the Internet while maintaining privacy, security, and anonymity (when needed) has never been easier.