Tails Linux Operating System: 
Remaining Anonymous with the Assistance of an 
Incognito System in Times of High Surveillance

Maurice Dawson, University of Missouri-St. Louis, St. Louis, MO, USA
Jose Antonio Cárdenas-Haro, California State University, Bakersfield, CA, USA

ABSTRACT

After the information released by Edward Snowden, the world realized about the security risks of high surveillance from governments to citizens or among governments, and how it can affect the freedom, democracy, and peace. And organizations such as WikiLeaks has shown just how much data is collected to include the poor security controls in place to protect that information. Research has been carried out for the creation of the necessary tools for the countermeasures to all these surveillance. One of the most potent tools is the Tails system as a complement of The Onion Router (TOR). Even though there are limitations and flaws, the progress has been significant, and we are moving in the right direction. As more individuals and organizations fall under a watchful eye on their Internet activities then maintaining anonymity it not only essential for getting out information but one’s safety.

KEYWORDS

Anonymity, Cyber Security, Intelligence, Linux, Tails Linux Operating Systems, TOR

INTRODUCTION

The erosion of privacy in the Web has created a movement from the free software advocates, in the search and development of free and proper tools for everybody. The TOR project is the core of this movement, followed by other many tools which are part of The Amnesic Incognito Live System (Tails). In this document is analyzed the importance of Tails and all its tools in the fight for privacy, freedom, and democracy.

THE BIRTH OF PUBLIC TOR

TOR project was set by the government and developed by the Defense Advanced Research Projects Agency (DARPA) as a security measure to avoid national and international surveillance of the classified government operations (Fagoyinbo & Babatunde, 2013). The Onion Routing principle is the use of several layers of encryption to conceal a user’s location and ensure private and anonymous
communications. Every router in this network only knows the address of the previous router and the address of the following one (Reed, Sylverson & Goldschlag, 1998).

Later the TOR project was released as a free software, and the development continues with funding from diverse sources (Tor: Sponsors, 2010); and these give more confidence to the public about its independence and reliability. So the use of this secure network soon became very popular in all the world propitiating its grow in many users and routers as well. The development of this project is continuous and dynamic; we are now in the second generation of TOR (Dingledine, Mathewson & Syverson, 2011).

This network was made available as a protection of the individuals’ privacy (which is a constitutional right in most countries), and to promote and maintain the freedom of confidential communications through the Internet among the public, avoiding or, at least, making very hard the monitoring of them. TOR is an excellent tool not only for the hide of political activists but also for domestic violence survivors to escape abusers (Russell, 2014), or just for regular users to bypass censorship (Gurnow, 2014).

The National Security Agency (NSA) has said that TOR is “the King of high secure, low latency Internet anonymity” (The Guardian, 2013). The TOR project received an award for projects of social benefit from the FSF (Free Software Foundation) in 2010, acknowledging it not only for the privacy and anonymity that it provides, but also for the freedom of access and expression on the Internet granted to millions of people, which has proved to be pivotal in dissident movements around the world (FSF, 2010). The Business Week magazine has described it as one of the most effective means to defeat surveillance around the world (Lawrence, 2014).

**HOW IT WORKS**

The more people using TOR network, the better. It is easier for a person to be anonymous among many others, it is harder to keep track of someone in a busy unknown and highly tangled network that is frequently changing and mixing up the connections randomly (Edman, Sivrikaya & Yener, 2007). As an analogy, we can say that a chameleon to camouflage effectively needs leaves, branches and trees, the more, the better for the blend. In defeating surveillance, we need to take care of several aspects. Who we talk to and when is just as important as what we said, and to secure these we also need encryption and randomness in the routing as well. The messages from the different anonymous users are shuffled and then sent to the next randomly selected router, shuffled again and so forth until the final destination is reached. So as an observer it is very hard to know which data were coming into the TOR network corresponds to which data coming out of it.

All the data is encrypted, including the origin and destination IP addresses, every time before it is sent to the next relay of the anonymous circuit. Since the TOR is a dynamic network that is constantly evolving, the path that our packets take to change all the time making things harder for the observer (Dingledine, Serjantov & Syverson, 2006). The users can set up a browser, a relay, a hidden service or all of them. Also “bridge relays” can be used to circumvent any blocking to the TOR network.

**THE NECESSITY OF ANONYMITY AND CYBER SECURITY**

We all need privacy for many diverse reasons, and is not only about the individuals, but also the private companies and even the governmental entities in the world need some anonymity at different levels. Journalists who want to protect their sources, or the law enforcement agencies that require communication with their infiltrated personnel in criminal groups protecting their identity, or the human rights activists in oppressive regimes, or the private companies in avoiding the disclosure of their technological developments for economic reasons, or the governments saving a lot of information for national security.
The Cyber Talent Gap and Cybersecurity Professionalizing
www.igi-global.com/article/the-cyber-talent-gap-and-cybersecurity-professionalizing/210627?camid=4v1a

Making IoT Run: Opportunities and Challenges for Manufacturing Companies
Peter Schott, Torben Schaft, Stefan Thomas and Freimut Bodendorf (2017). International Journal of Hyperconnectivity and the Internet of Things (pp. 26-44).
www.igi-global.com/article/making-iot-run/201095?camid=4v1a