Chapter 10
Tails Linux Operating System:
The Amnesiac Incognito System in Times of High Surveillance, Its Security Flaws, Limitations, and Strengths in the Fight for Democracy

Jose Antonio Cardenas-Haro
University of Missouri – St. Louis, USA

Maurice Dawson
University of Missouri – St. Louis, 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/or peace. Research has been carried out for the creation of the necessary tools for the countermeasures to all this surveillance. One of the more powerful 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.

DOI: 10.4018/978-1-5225-0741-3.ch010

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).