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

Maurice Dawson
Jose Antonio Cárdenas-Haro, California State University, Bakersfield
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 ANON YMITY AND CYBE R SECUR ITY

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.
Surveillance and Espionage have always been an issue; several countermeasures have been developed according to the times, but now is harder than ever. The cell phones can easily be converted into tracking devices and recordings of the phone calls, web pages visited, Internet search history and interactions in social media can create a detailed profile of anyone. The persons can be affected negatively by all these. They could suffer work discrimination because of their political views, or even their physical integrity could be in danger for those who are living in tyrannic regimes, like the recent case of Niloy Neel a Bangladeshi blogger killed in Dhaka (BBC, 2015). The governments are always looking for ways to have more control and capabilities for surveillance; Linus Torvalds, the creator of the Linux Operating System (OS) and still in control of the development of the Linux kernel, revealed that the NSA asked him to put a backdoor in the OS (Greenwald, 2014).

Furthermore, there is the high risk of a democracy degrading into an authoritarian state if its citizens are surveilled to the degree of losing their privacy. The government can face significant economic risks if sensitive information is leaked, as in the case of the tax accounts hacked in the IRS (Weise, 2015). The use of technology is increasing and spreading quickly in most of the devices used by humans, which represents a new security threat if the owners lose the control of them, as in the case of the car hacked when in the middle of the road (Ward, 2015). For all these and more, the governments and the citizens are always looking for ways to avoid the intrusion in their data and systems.

BIRTH OF TAILS OPERATING SYSTEM

The first version of the operating system The Amnesic Incognito Live System (Tails) was released in mid-2009 as a merge of the Incognito and Amnesia Linux distributions. It was created by a team of anonymous hackers which still are in charge of its development, with support and funding from the TOR project and the Freedom of Press Foundation (FPF) (Finances of Tails., 2015), and also from the Debian and Mozilla projects (Tails report, 2014), and other sources that continue founding it. The Tails project is based on the Debian distribution with the security and anonymity as a core philosophy to give privacy to anyone anywhere. Tails were born as a complement of TOR to enhance the anonymization of their users. The Tails Linux distribution became so famous after being known that is the OS used by Edward Snowden, the whistleblower who leaked information about the PRISM project to The Guardian and The Washington Post newspapers (Finley, 2014). The Tails team created this Linux distribution as a countermeasure of erosion of online privacy. The big companies of the Internet, as well as the governments (especially in totalitarian regimes), want to take away our privacy making our lives more transparent every time.

THE STRENGTHS

The Tails OS is an integrated system consisting of several tools aimed to avoid the detection of the identity of their users. It is designed to boot from a removable live media as a Universal Serial Bus (USB) stick or a Digital Video Disk (DVD), and the saving of any file in it is deleted after a reboot for security reasons; of course, we can use the hard drive or another USB memory for the saving of the required data. In the case when we really want to delete any document, videos, pictures or any data file, the Tails is equipped with a tool called “Nautilus Wipe” for securely deleting the data; this is necessary since regular operating systems only remove the file name and link from the file system directory, not even the reformatting or overwriting of the hard drive or memory stick is a guarantee that the deleted or previous information is indeed gone. Tails come with visual camouflage that can be activated to give the look and feel of a Microsoft Windows 8 system, the purpose of this is to avoid attracting unwanted attention when working in public places.

All the traffic is handled through the TOR network, using Media Access Control (MAC) spoofing; all these to avoid leaving any digital footprint. It also gives the option to use Invisible Internet Project (I2P) as an alternative to TOR. The I2P is an anonymous overlay network used as an instrument to
circumvent surveillance and censorship. This Linux distribution includes several state-of-the-art cryptographic tools to encrypt files, emails and instant messaging. It uses LUKS Linux Unified Key Setup (LUKS) which is an encryption tool for hard drives or USB sticks. All the communications with websites are encrypted automatically using Hypertext Transfer Protocol Secure (HTTPS). In the case of documents and emails, are encoded using Open Pretty Good Privacy (OpenPGP). The chatting or instant messaging is done using Off-the-Record (OTRP messaging which is another tool for encryption which also provides deniable authentication that cannot be achieved with PGP systems (Borissov, Goldberg & Brewer, 2004). It includes the “Shamir’s Secret Sharing” program which runs an algorithm used in cryptography where the decryption of a message is only possible with some threshold number of participants (Shamir, 1979).

Tails also come with software to create virtual keyboard as a countermeasure against hardware keyloggers, and even with tools to anonymize metadata in files, to calculate checksums. It includes the “AppArmor” system which is a Linux kernel enhancement to confine programs to a limited set of resources. To prevent the “cold boot” attacks and forensics to the Random Access Memory (RAM), it deletes all the memory at the shutdown.

The updates to patch any security hole are available in a prompt manner as an automatic mechanism to upgrade the USB stick or the Secure Digital (SD) card to the most recent version of Tails. The creators of Tails and TOR support and promote the search for flaws in the system as a way to keep it in a continuous improvement state. This incredible operating has been created using only free software, which is a must in these cases since closed private software cannot be trustable. It is not a coincidence that Tails is the preferred operating system by Edward Snowden (Finley, 2014).

APPLICATIONS FOR ANONYMITY

Tails has many software included for networking, encryption, and privacy. This OS can be run as a Virtual Machine (VM), LiveUSB drive, or directly installed on the native machine. There are no associated costs with Tails which is great as this is yet another level of protection ensuring there is no financial footprint associated with the use of this OS. Tails has an application that allows for the creation and management of encryption keys for emails. Figure 1 displays the Tails OS running in a

Figure 1. Tails Desktop in Oracle VirtualBox
virtual environment. The use of encrypted storage devices, key signing, strong password generation, removing identifying metadata in files, and more add to the over security. The removable of the metadata is important because Open Source Intelligence (OSINT) can be done which can provide data such as geolocation, time stamps, and more. Further, text can be used to create a behavioral analysis profile on subjects. A software application such as Maltego can scrap the web for any digital footprint to create a link analyses from tweets, email messages, and more.

Since this OS is Debian based all software packages available for Debian can be installed in Tails. However, this would be cautioned unless a source code scan in conducted to see what Common Weakness Enumerations (CWEs) are in the system of origin. Once these CWEs have been addressed to an acceptable level, then that particular software application can be installed. Additional packages can break the security of this OS. Thus to do this would require the creation of a secured installation script. In Figure 2, an example is shown that could be written to provide those needing additional application the ability only to run already whitelisted program that does not affect the security posture of Tails.

Bitcoin is a peer to peer electronic cash system that no one controls, and there are not printed currency (Nakamoto, 2008). In Tails included, is Electrum which is a Bitcoin wallet. This application is a lightweight wallet that connects to external user’s to query blockchain data. Bitcoin allows the exchange of goods or services with some level of anonymity. In turbulent economies where currency continuously falls this currency could be the method used to ensure organizations are not being financial undermined by nefarious entities (Osterrider, Strika, & Lorenz, 2017).

LIMITATIONS AND FLOWS

As is the case with everything, the Tails system has its limitations. This system is the conjunction of many tools, any flaw in any of its tools becomes a flaw for the Tails system. Furthermore, working effectively under this system requires some technical knowledge, most of the tools in Tails are not precisely user-friendly. It is known that the NSA has been able to crack the computers of some TOR users, but not the core security of the TOR network (Ball, Schneier & Greenwald, 2013); this has to

Figure 2. Sample Installation Script
do more with errors or carelessness from the users. Tails were created as a complement to the TOR browser, as an integrated system for the improvement of the security and anonymity.

TOR encrypts all inside its network and anonymizes the origin of the traffic, but the communications from the TOR network and the final destinations are like the regular transferring of information on the Internet. So, depending on your data, you might need to use some of the tools provided in Tails for further encryption and authentication. Also, we need to change some of our habits, it is not recommended to enable or install browser plugins, neither to open any document downloaded through TOR while online. The Tails does not protect against compromised pieces of hardware, like a key logger unless you use for this specific case a virtual keyboard “Florence” provided in one of its tools. The Basic Input/Output System (BIOS) or firmware attacks are other forms of compromised hardware.

Another important factor that needs close attention is the metadata in our files. Tails does not clear it for us, but it provides the tools necessary for the removal of information that can help to identify us from the metadata, before sending any of the files. In the case of e-mails even if we encrypt the contents, the subject and other headers remain understandable. Another problem in the case of TOR is that it does not protect us from a global adversary, this means an entity monitoring all or most of the nodes in the TOR network, such entity using statistical data may infer the relations between the users and the connections (Dingledine, Mathewson & Syverson. 2004). Another important habit here is the use of a strong password, and the Tails will not create strong passwords for you. It is not straightforward to hide the fact that you are using Tails, and this in some ways is a disadvantage, a flaw in the anonymity. Users have to be ready to update the Tails system every time that there is a patch available.

QUESTIONABLE GOVERNMENTS

Some governments have suppressed the ability to freely communicate and present non-biased news to the public that may not be to the current party holding power. Some countries have been found using FinFisher’s FinSpy application which intercepts and records a variety of information (Dawson, 2015). This software application has been found within the hands of over twenty governments that have questionable records on human rights (Pelroth, 2013). The FinSpy software was used in Ethiopia to target political dissidents. In Morocco, there have been reports of the government using the Internet to monitor its citizens. In Tunisia Internet censorship and control has been in place since it was publicly available in 1996 (Wagnner, 2012). These activities have repeated in authoritarian and corrupt governments.

TOOL FOR FREEDOM AND DEMOCRACY

As humans, we have the natural right to privacy and in all the democracies that right is granted in the constitutions. Unapproved or unreasonable searches and seizures go against the human rights. The exchange of information between individuals, corporations or governmental agencies has to be encrypted. It is evident that would be easier for the cops and law enforcement agencies to detect illegal activities if the information were not encrypted, but in the same way it would be easier for the criminals to affect the citizens.

The open source philosophy is a great medium to provide trustable tools to build all the infrastructure that we need to keep the freedom and democracy not only on the Internet but also in our lives. The open source has given birth to the Linux operating system, encryption tools, Wikipedia, Wikileaks, Bitcoin, BitTorrent, social media and many more valuable programs. The General Public License (GPL) is a free software license to guarantee anybody the right and freedom to use, modify and share the programs (Dawson, Leonard, & Rahim, 2015). All these show how humans around the globe can be organized without borders to improve their economies, to build the required products
without the need of the private companies or centralized governments with all the toxic and corrupted control that they represent. In other words, out of the master and slave model, or without “baby sitters”.

The mistrust of a central authority is common anywhere, as humans, we have the innate desire for freedom in everything. It is important to clarify that while some media and governments have slandered and libeled the DarkNet, the TOR, and the Tail Linux OS saying that these are evil tools used by criminals; all these are also essential tools used by many people for the good, including dissidents, journalists and law enforcement agencies around the world.

There is always the risk of cyber espionage or mass surveillance done by governments around the globe. In the case of US is with the project PRISM developed by the NSA (Ball, 2013). The UK has the project Tempora (Bump, 2013). In Russia is the SORM project (Paganini, 2014) and China has two significant tools for the control of the Internet, the Golden Shield (or Great Firewall) for censorship and surveillance (Randy, 2009); and the Green Dam for Personal Computer (PC) content control (Watts, 2009; Chen, 2009). There are also companies that sell technology for surveillance even to oppressive regimes (Gilbert, 2015), so we can say that all or, at least, most of the states around the world do some kind surveillance that could go worst as the technology improves and evolves. The monitoring between nations can cause tensions and damage in the diplomatic relations or even the loss of them (Smith, 2014; Menn, 2015; Fitsanakis, 2013).

Furthermore, the surveillance does not come only from the states. The private companies also want your data for economic purposes. They want to know what are you more likely to consume, to buy, and this way you could become the target of some specific advertising. Companies like Microsoft, Apple, Facebook, Yahoo, Google or Amazon among others are collecting their user’s data is also for psychological manipulation to make you consume some products that other way you might not buy. They need all the possible information from you to link it with your real life behavior, and these give them some control over you. Your cell phone location, who you share information with, who you talk to, what you buy, etc. The companies usually have arrangements with the government to share this information or they might also be under government surveillance for these data (Branstetter, 2015; Greenwald, MacAskill, Poitras, Ackerman, & Rusche, 2013; Bekker, 2013). The problem is that the more you are surveilled, the less autonomous and free you are. It is not easy to know the level and kind of control that they could exercise over us, but our freewill is indeed affected.

People are saying that they do not care about surveillance because they do not have anything to hide pure ignorance, it is like saying that they do not care about free speech because they do not have anything to say. Thanks to free thinkers and researchers, there are tools, services, protocols and free software available and under continuous development and improvement to avoid surveillance, for an anonymous and private exchange of information; science and technology is fighting back. All these come down to live a free life which is a core human value, and a foundation for any true democracy.

**CONCLUSION**

As more people express the desire for privacy, the demand will fuel the market as data found publicly can fall prey to those conducting OSINT mining and analysis for bad reasons. By making the surveillance harder we protect ourselves as individuals, and all the others by making it more expensive to monitoring everyone all the time. At the end encryption and chaos is all about mathematics, and in the quest for more privacy, the numbers work in our favor. It is a lot easier the encryption of the data than the decryption of it for intruders. Our universe fundamentally prefers privacy. In order of having a free society, we need to have freedom from analysis about behaviors and communications among us. When considering issues of privacy, cyber terrorism, and digital crime it Tails allows us to navigate freely, safely, and securely (Dawson & Omar, 2015; Dawson, Omar, & Abramson 2015). In our hyperconnected society, it is imperative that anonymity is maintained during certain actions because of misuse and abuse.
REFERENCES


Branstetter, B. (2015, August 16). The NSA is asking your favorite apps how to spy on you better. *Business Insider*.


Lawrence, D. (2014). *The inside story of Tor, the best Internet anonymity tool the government ever built*. Bloomberg Businessweek.


Russell, B., (May 2014). Domestic violence survivors turn to Tor to escape abusers. *The Verge*.


---

*Maurice Dawson is an Assistant Professor of Information Systems at the College of Business Administration at University of Missouri- St. Louis with affiliation to the Cybersecurity and Information Technology Innovation Lab (CITIL). He is currently a Visiting Professor at the Polytechnic University of Puerto Rico, Visiting Professor at the University of Nairobi, and a Senior Research Fellow at the American Leadership & Policy Foundation (ALPF). Additionally, he was a Visiting Assistant Professor (Honorary) at the University of Tennessee in the College of Engineering within the Department of Industrial and Systems Engineering. Dawson has received a Fulbright Specialist Grant to Russia in 2014 to South Ural State University. Dawson served a Visiting Scholar with the University of The Gambia through the International Studies and Programs (ISP) Fellowship awarded from the University of Missouri Systems (UMS) in 2014. Dawson received an appointment as an International Business (IB) Research Associate in the UMSL International Business Institute (IBI). He is currently completing a second PhD at London Metropolitan University in the Intelligent Systems Research Centre (ISRC).*

*Jose Antonio Cárdenas-Haro received his PhD in Computer Science from the Arizona State University (ASU), his Master’s in Computer Science was granted by the Ensenada Center for Scientific Research and Higher Education (CICESE), and he also he holds a BS in Electronic Engineering from the Technological Institute of Los Mochis (ITLM). His research interests include parallel and distributed computing, algorithms, network security, cyber security, bioinformatics and applied mathematics. Cardenas is currently working in the Computer & Electrical Engineering department at California State University, Bakersfield.*