Association for Information Systems
AIS Electronic Library (AISeL)

2017 Proceedings | Portugal (CAPSI)

2017

Paranoid operative system methodology for anonymous & secure web browsing, doctoral project

Nuno Mateus Coelho
Universidade Trás -os-Montes e Alto Douro, al63826@utad.eu

Benjamim Fonseca
Universidade Trás -os-Montes e Alto Douro, benjaf@utad.pt

António Vieira de Castro
Instituto Superior de Engenharia do Porto, avc@isep.ipp.pt

Follow this and additional works at: http://aisel.aisnet.org/capsi2017

Recommended Citation
Coelho, Nuno Mateus; Fonseca, Benjamim; and Castro, António Vieira de, "Paranoid operative system methodology for anonymous & secure web browsing, doctoral project" (2017). *2017 Proceedings*. 10.
http://aisel.aisnet.org/capsi2017/10

This material is brought to you by the Portugal (CAPSI) at AIS Electronic Library (AISeL). It has been accepted for inclusion in 2017 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

Paranoid operative system methodology for anonymous & secure web browsing, doctoral project

Nuno Mateus Coelho, Universidade Trás-os-Montes e Alto Douro, Portugal, al63826@utad.eu
Benjamim Fonseca, Universidade Trás-os-Montes e Alto Douro, Portugal, benjaf@utad.pt
António Vieira de Castro, Instituto Superior de Engenharia do Porto, Portugal, avc@isep.ipp.pt

Abstract

Recently the world knew by the media, that its leading nations follow closely their citizens, disregarding any moral and technological threshold, that internal and external security agencies in the USA and Europe closely follow telephone conversations, e-mail, web traffic of their counterparts, using powerful monitoring and surveillance programs. In other corners of the globe nations in turmoil or wrapped in the cloak of censorship persecute and deny uncontrolled web access without harmful repercussions to their citizens.

This work is a research-in-progress project and consists in showing the research done so far to develop a methodology. This consists in the construction of an operative system with an academic scientific source that permits a secure and anonymous use of the web. For such methodology, first is required to comprehend and get acquaintance with the technologies that controls usage of web consumers, solutions that enable and grant some anonymity and security in web traffic.

Keywords: tor; anonymous; linux; web; methodology

1. INTRODUCTION

We live in a time when society is challenged by the sudden changes in social, political and economic levels, all of them with heavy environmental costs. This strong volatility implies consequences in terms of (in)security of societies and organizations. The speed at which succeeding events, new technology offerings, trends, products, problems and solutions creates a disarray that is already, and despite the efforts of those who regulate, virtually impossible to contain or hide. Research and massive use of information and social sharing were created by the advent of Web 2.0, or the 2nd generation of the web, a term introduced by Tim O'Reilly (O'Reilly 2009), which associated with the new generation, web 3.0 characterized by the Semantic Web, a term introduced by John Markoff (Murugesan 2009), creates a unique singularity comparable only to the human ecological footprint. The human digital footprint means that everything that is shared and exposed in the online, will be stored somewhere in computer clusters with an estimated useful life time impossible to calculate, thus accessible to others for many generations to come. By relying on Cloud platforms (data storage in virtualized computing clusters) to publish and store

ISSN 2183-489X
DOI http://dx.doi.org/10.18803/capsi.v17.127-143

personal information in social networks a door was open to cybercrime (crimes committed using information technology) which for years was directed to organizations.

2. CONTEXT

In 2014, and according to Internet Live Stats (Internet Live Stats 2015), about 3 billion users were connected to the web and sharing data. The web is extremely conducive to all kinds of harmful acts committed by strangers. Because it is a living entity (in the broad sense of the word), this globalization, this network made up of people and machines is also a source of misinformation directed to nations that compete with each other. For these entities, who first holds the validated information has in fact the lead and to achieve it, whether this is economic or strategic, creates mechanisms that advocate the computer insecurity through decoding, modification and information interception to retain it for their own benefit.

Computer security is tested constantly. According to Paulo Santos (Santos and Bessa 2008), from information pirates, commonly known as hackers to government security agencies, everyone wants a piece of the *El Dorado*. Computer systems connected by network and, above all the wide network that is the web, are used to store and manipulate information daily by millions of people and organizations. According to Herman Walker (Walker 2009) schools, universities, doctors' offices, students or teachers, all of them and all these entities exchange information using computer networks; now, it is safe to say that the information is in circulation, and therefore it is critical maintain this logistic infrastructure and content secure.

The computer security is increasingly a social problem and technical problem. Technical because the variety of systems, standards, architectures, methodologies, make the task of implementing measures and safety standards, risk mitigation circuits and development of computer master plans that anticipate and respond to unexpected questions, a real daunting task. This results in the inability to create a complete coverage of effective security policies. Adding to the equation the connection to distributed systems and to the web, it becomes an impossible task (Lopez et al., 2015).

Social problem, because the non-technical users of these systems lack the sense of existing security issues. For these, according to Brian Shea (Shea 2009), is transparent all the effort and systems behind the screen, disregarding great attention to detail because they feel safe by having an antivirus, or a firewall that sends graphic alerts in the GUI (Graphical User Interface). They also rely in the in-the-house (company support technicians) or paid support to implement measures and help them in daily difficulties.

Applications aiming to exploitation and the lack of attention from the public or system administrators is developed on a daily basis. Also, reputed companies develop and launch to

market applications to allow avoidance of mechanisms that insist on violating computer privacy. Time-over-time software was created with the propose of maintain the security of information and their users. Entities such as Symantec (software and computer security company) daily release updates to their antivirus programs in response to new threats. Companies like Microsoft creates updates regularly to fix bugs and software vulnerabilities like the SMBv1 bug. Companies such as CISCO develop network appliances (equipment) subject to adjustments, and other features that are not adjustable in order to standardize concepts of security and defence mechanisms (Shelly and Campbell 2014). Despite this panorama these measures are reactive to daily challenges and unfortunately not preventive.

2.1. The Problem

According to Symantec, in the report of Insecurity of Internet of Things, in 2016 were estimated to be connected to the web approximately 4.9 billion devices (Barcena and Wueest 2014). Many of these devices concentrate itself few active and passive safety mechanisms as is the case of mobile phones, tablets and smartphones. Regardless of this outlook every day millions and millions of users share information and data through these devices. Currently organizations have ceased to be the direct target of those dedicated to theft and misuse of information. The average user has become a target because the amount of information shared online without having a sense of their digital footprint. Also attacks on systems that provide services such as Web Servers that store information about users are under fire. In May 2015, the alleged attack on the online Portuguese lottery platform *EuroMillions* was reported by pplware.sapo.pt website in (Bessa 2015). According to them data from 20,000 users was compromised. The attack shape was not disclosed but information was exposed and may be used for future attacks. The information revealed consisted of usernames, hash, MD5 (Message Digest 5), salt, emails and birth dates. Although this data may seem unimportant, these elements allow intrusion attempts into email accounts that have birth dates as password, and the possibility to retrieve a new password from the *Euromillions* website, after using the security mechanism that uses procedures like questions or confirmation of dates. The year 2013 was rich in revelation of events and activities of North American security principals. According to revelations of Julien Assange (Assange 2013) in WikiLeaks (online platform for sharing information), secure web browsing does not exist and even the location of users is not safeguarded. According to the same author several countries could access the user data and extract relevant information.

There are countries for its political characteristics enforce rigorous control of content available in the web. According to Ronald Deibert et al. (Deibbert et al. 2008), countries like North Korea, Iraq and Syria limits access to physical and technological level, e.g., only certain people may have access to devices that allow access to the web, and still must go through a barrier imposed by ISP

(Internet Service Provider(s), e.g. Portugal Telecom). This inhibits them to view content from certain sites, countries, religions, etc. The world most notorious case of this is the Great Firewall of China, also known as Golden Shield Project.

3. THREATS AND COUNTERMEASURES

As the expansion of worldwide networks advances in a very fast rate, information security and privacy begins to be seen differently. Keeping safe the information and telecommunication systems plays a vital role in the day-to-day actors of this panorama, may them be users, systems administrators in domestic, business or government environment.

3.1. Threats

According to Paul O'Day in the Journal of Education at Pacific University (O'Day 2013}, the North American Government controls the web since its appearance. Its military genesis puts government institutions in a privileged position relatively to others. The most effective way to compromise the security is listening and penetration to the ISP before the data arrive at the destination computer. If communications and connections are not encrypted, it's possible to find out the location, content, information about the computer and above all know specifically who the user is (Locati 2015). Until recently it was not known that the NSA was spying in Internet users at national and international level.

Threats are not only from governmental source or about secret societies. It is also a harmful and lucrative criminal activity, a reminder to existing computer problems on platforms or systems, a source of information that allows third parties to obtain a relevant position by using information. According to Eric Raymond (Raymond 1996), and according to Robert Moore (Moore 2014), there is a group of people who recurring to the use of high computer skills with very specific goals, are dedicated to increase their knowledge exploring, modifying or accessing systems that they normally don't have access to.

The censorship that controls large populations is also reality nowadays. The Golden Shield project and others like so, according to Sarosh Kuruvilla et al., (Kuruvilla et al. 2011), appeared after the arrival of the Internet in 1994 to China. The Chinese government in 1997 set in motion the first control measures issuing regulations in the use of the web and appropriate penalties. In 1998, the Communist Party, for fear of losing control of the country instructed to be created and implemented a system able to control the entire web traffic network. Nicknamed the Great Firewall of China in 97, employs more than 45,000 policemen and is a network of complex proxy servers to prevent the IP of Chinese origin to get out by others than the Six Chinese Gateways, thus controlling who accesses what, and what is available to access.

3.2. Countermeasures

Effective security is expensive and evaluate it is an arduous task out of reach of those who normally can unlock funds for the ones who decide the implementation of security measures. In computer science, there are two areas where there are no solutions that responds to 100% of the problematic: computer security and software testing (Boavida et al. 2013).

3.2.1. Information Security

Behind any tool or equipment that ensures security or the behaviour that a given technology must adopt as guidelines, there is the concept of policies and politics. These perform as standards to many services, systems and technologies with the objective of governance, maintenance and securing information. In information systems exists a mandatory mantra to enforce and comply security, vastly applied in politics and policies that enforce fault defence capacity, defence against catastrophes and non-authorized activities. These decrease the risk of passive and active attacks recurring to modification, spoofing, denial of service, repetition, message interception and repudiation (André Zúquete, 2014), they are:

- Integrity – Guarantee that a given information is true and without non-authorized modifications over its entire life-cycle;
- Authenticity – Guarantee that a given information travels unaltered from the original sender over its entire life-cycle;
- Non-repudiation – Guarantee a that one party of a transaction cannot deny having received a transaction nor can the other party deny having sent a transaction;
- Availability – Grantee that a given information is always available when necessary recurring to techniques that can avoid failures, e.g., denial-of-service attacks;
- Confidentiality – Guarantee that a given information is only available to whom is authorized to access or view it.

3.2.2. Policies and Guidelines

The previous point are base stone for policies and guidelines such as ITIL[1], COBIT[2], ISO 27001:2013[3] and ISO 20000[4]. These exist as standards and serve as guidelines when adopted by entities that require security assurance for their systems, and for the people that interact with them.

[1] ITIL - Information Technology Infrastructure Library

[2] COBIT - Control Objectives for Information and Related Technologies

[3] ISO 27001:2013 - Information security standard that was published in September 2013

Resources like COBIT aim to provide effectiveness, efficacy, confidentiality, integrity, availability, reliability and compliance as business requirements, recurring to IT processes and IT resources. These are the dimensions of COBIT, and observable in the next figure:

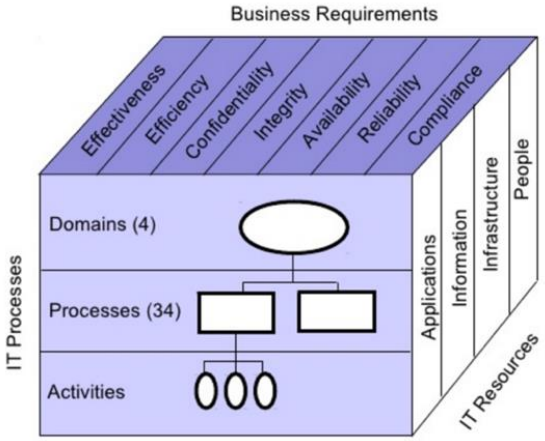

Figure 1 - COBIT Dimensions and levels cube.

As countermeasure, security polices play the most important role as they can be used as tool that define behaviours or tool that defines product or services definition in the architecture phase of development. Security policies provide a set of rules and standards that must be adopted and followed by users of computing resources in an organization and reflect the security objectives that the organization has outlined as the basic rule of security. These policies establish in detail the permitted uses for information and communication resources and systems, as they outline punishments in case incompliance or misuse.

Policies or information systems standards like ISO 27001:13 or ISO 200000 offers specific guidelines that reduces the security and management failure risk, they are:

- Be easily accessible to all members of the organization;
- Establish and define security objectives;
- Determine in concrete terms all aspects of its scope;
- Define the position of the organization in each question;
- Justify the options taken;
- Define the circumstances of individual application of the rules;
- Define the scope of action of the various agents of the organization;

[4] ISO 200000 - The first international standard for IT service management

- Outline the consequences of non-compliance with established rules;
- Define the level of privacy guaranteed to users;
- Identify contacts for clarification of dubious issues;
- Define the treatment of missing situations.

The document that defines the security policy should exclude all technical aspects of implementation of the security mechanisms, as each implementation can vary over time. In addition, this must be a brief document and easy to read and understand.

3.2.3. Security tools

All computer systems require access components or interfaces for users (clients). Whether these are via browser or server management console, all have a specific access having as the most important input port and possible damage, the administrator access. As a good practice for secure access, system administrators must have implemented in their systems a security protocols, such as Kerberos[5]. This protocol is very common in Apache systems (with *mod_auth_kerb* module), Mac OS (Apple operating system), SSH[6], SAMBAv3 (file sharing protocol in Linux) and Java systems since version 1.4. Keeping these accesses secure and encrypted is essential.

SSH - There are tools available to most users and free to use in most operative systems nowadays. These provide secure access to systems or services recurring to powerful protocols and encryption methods. From the many possible and available within the objective of this work the SSH will serve as example. It possesses three relevant components:

- Transport Layer Protocol – Provides authentication, confidentiality, integrity and compression if needed;
- User Authentication Protocol – Using the transport layer protocol authenticates the client with the server;
- Connections protocol – Multiplexes an encrypted tunnel into multiple logical tunnels, running over the User Authentication Protocol.

VPN - The concept of virtual private network (VPN) is nowadays used to identify several secure communication solutions. VPN is a secure extension of a private network over an insecure or public network such as the web. Regulated by the VPNC (VPN Consortium) manufacturers consortium, secure VPNs ensure that data security between sender and receiver is independent of

[5] Kerberos - The Network Authentication Protocol

[6] SSH – Secure Shell, https://pt.wikipedia.org/wiki/SSH

honesty, of the entities, of access and information routing, being a technology widely used in both business and domestic environments. One of the largest secure VPN networks in the world and fundamental component of the prototype and therefore of the to be designed methodology is the Tor network. There are also VPNs that are configured locally through software or hardware and there are global VPN networks that are marketed as services so that your users surf the web allegedly secure. In a way, a VPN acts as a virtual network cable, that is, there is no physical connection. However, as this virtual cable extends through the public network that is insecure, VPNs are endowed with security mechanisms that allow them to be effectively secure. The most common standards are IPSEC and SSL. IPSEC is an IP protocol security extension designed for IPv6 and applied to IPv4. SSL is a protocol created by Netscape to introduce security in HTTP communications.

Firewall - When connecting systems with the outside world, one should be zealous of all safety-related issues. A firewall system precisely and accurately controls all traffic and who has access to each IP port of a given system. The firewall is a device, a software service present in the operating systems, or software that determines the access control policy to or between networks, containing the following characteristics: All incoming and outgoing traffic must pass through the firewall, only data traffic allowed through local security policies can pass the firewall without being dropped, the firewall must be immune to penetrations. In Linux, for example, there are three types of firewalls: Ipfwadm, Ipchains and Iptables. The use of in depth firewall (in depth as in a cascade style, as one firewall secures a perimeter allowing the access to a lower one where another firewall exists), prevented the most recent global ransomware attack WannaCry 2.0 [7]in Vodafone Portugal (Coelho, 2017)

Cryptology and Cryptography - From cryptology, the cryptography that originates from the Greek *kryptós,* whose meaning is hidden, and *gráphein* which means to write. It is a computer science that studies the methods, mechanisms and algorithms by which a message is transformed from its original form to an unrecognizable one unless the key is known that will help make the message perceptible. Cryptoanalysis is the method of study that aims to obtain the message or the information of the encrypted message without having the key that decodes it. The classical methods of cryptanalysis are:

- Brute Force - A method of testing all possible character combinations until you find the key that will enable decoding of the message;
- Frequency analysis - A method that is based on the fact that in some languages, certain characters or combinations occur more frequently.

[7] WannaCry - A ransomware computer worm that targets computers running Microsoft Windows.

The main purpose of cryptography is to ensure that the exchange of data between actors, transmitters and receivers satisfies the basic principles of security. For this to be possible the use of ciphers is the key. The cipher is the cryptographic algorithm, an injective mathematical function that effects transformations between the original text and the coded text (cipher) and vice versa. The cipher algorithm is essentially a set of procedures on which cryptographic techniques are based. The keys to these algorithms provide information to apply these procedures in a unique way, with three types of keys being known: the secret, the public, and the private. The secret key is also known to be the symmetric key; On the other hand, the public key is also called asymmetric. In the use of a symmetric key to encode or decode a message, the sender and the receiver need to choose a cipher and a key, the sender encoding the message and the receiver deciphers the same. The algorithm defines the generic model of data transformation and the key is a parameter of the algorithm that allows to vary its behaviour in a complex way.

Secure Operative Systems - There are multiple operating systems that give more or less security to the user. There are commercial systems commonly seen in x86 and x64, which stand out for their beauty and leave the computer security in charge of vendors that trades applications for these systems. While this is the reality, when it comes to the prestige of a software the manufacturers brands rush to launch corrective and preventive packages without the support of their business partners (Panda, Symantec and others).

Currently, most secure operating systems are Linux based and are known worldwide for their quality because they are equipped with the latest software that every day is studied, so that user safety is always in the first level. In fact, the best countermeasures to the identified issues are available to the public in the form of secure operative systems, or to the author, paranoid operative systems. Systems developed by entities that aim to be in the front row of security for personal users and companies. These consist in Secure Operative Systems (OS) with unknown or not clear origin that do not collect or keep user's data, do not need a common hardware platform, and run over a virtual machine or Live DVD at start-up from the DVD tray (drive).

Some of these platforms are completely open source and others not, but, generally they are good and under the scrutiny of the most knowledge users worldwide. Despite this, the most renowned have a dubious origin as they emerge from within small groups of developers, and the steps engaged to construct them or its effectiveness lays in secret. The most acceptable by the open source community can be analysed in the Table 1.

Name	Architecture	Origin
Tails – The Amnesic Incognito Live System	Linux Debian LiveDVD 86x and 64x	The Tor Project, Inc
JohnDo Live DVD	Linux Debian Live DVD 86x and 64x	Academic institutions
UPR-Ubuntu Privacy Remix	Ubuntu Live DVD 86x and 64x	Private group

IprediaOS	Ubuntu Live DVD 86x and 64x	Unowned community
C3PIV Portuguese Unique Initiative	Portable APPS Windows environment only	Portuguese university consortium

Table 1- Secure Operative Systems

Tails - The Amnesic Incognito Live System is based on the Linux Debian operating system, with the motto of privacy for everyone everywhere, this operating system is known for its paranoid orientation (designation that gives operating systems that greatly value security and anonymity) and for being extremely secure and versatile. In order to preserve privacy and anonymity, it helps in the use of the web anonymously and can avoid the censorship imposed by known firewall systems, without leaving a trace unless users specify it. Its origin is from the The Tor Project, Inc, the owner of TOR network. Despite the owner of this tool, it lacks the information of its composition and the criteria used to select it among others. It differs with the preponed methodology because it allows installation in a hard drive.

JohnDo Live DVD - Developed initially by the University of Dresden, by the University of Regensburg in Germany under the name JAP (Java Anon Proxy), the now JonDonym is very similar to Tails in operating system distribution mode; However, this product stands out as a commercial version of computer security. Seated on a network of proxy servers, they function similarly to Tor with two levels of service provision, free and premium (enhanced version), which encrypt the information at each pass of information by each node. JonDonym is based on a principle different from P2P (peer to peer or peer-to-peer) networks on which Tor and I2P are based by maintaining their anonymous nodes. Unlike Tor that establishes a VPN network distributed by all servers anonymously, this version claims to be more reliable because there is 100 percent certainty of the node property. In the Tor network, any citizen can program and make available an access or outgoing node to the unencrypted network, making the system potentially vulnerable if less reliable entities decide to create their nodes in order to analyse the traffic. The fact of its commercial intention makes this tool inaccessible to most people. The propose methodology consists in the empowerment of its users to bulk up their operative system with specific tools, free and open source.

Ubuntu Privacy Remix - Coming from Germany, Ubuntu Privacy Remix is an Ubuntu / Linux based operating system based on the pillars of security by isolation and Air Gap. The goal is to provide a completely isolated network communications operating system. It aims to provide a controlled environment so that sensitive information is always contained within a specific circuit where only encrypted devices can be used to transfer information. In a non-installable form, this LiveDVD prevents unauthorized access to the system, reducing the risk of theft or loss of information by conventional means of malware, trojans, viruses and unauthorized access. According to the UPR website, from the reports of Edward Snowden it became clear that

government entities closely follow the Internet users so the tool avoids this because, in addition to being impossible to adjust or configure the basic security settings that are already preconfigured, All Lan, Wlan, Bluetooth, infrared, and point-to-point (PPP) network support have been removed from the modified kernel of this distribution. This type of technique may seem simple to implement just by disconnecting from the wireless network card; However, there is software capable of turning the support on and off without the user noticing. Profoundly different from the proposed solution. This operative system relies in Bruce Schneider's ideology of Air Gap, thereof, it does not connect to the web. Its last version is from 2013 and was now (2017) replaced by a new one called Discreet Linux lacking extensive peer review.

IprediaOS - Ipredia OS is an extremely functional, fast and stable operating system. Based on a Fedora Linux distribution it provides an anonymous browsing solution including email, chat and online file sharing. Contrary to the solutions discussed above, this version doesn't use the Tor network for encrypted communications but rather the I2P protocol to allow the anonymity of the user through its VPN network. This solution allows its installation as well as the use in LiveDVD, being only desirable to choose the desktop Gnome or LXDE GUI. In the latest version and available for download, a wide range of tools is provided to the user ranging from Bit Torrent client, text editor, calendar, PDF viewer, email client, among others, properly safe. A secure chat system, IRC via the I2P Network and the Firefox browser are also available for anonymous browsing. The use of this tool as LiveDVD can be used in complete safety and can also be installed directly on a possible user's computer. This solution allow installation and therefore vulnerable to a ransomware attack or possible incrimination of its user.

C3Piv – Originally with the motto of providing common users with a tool to respond to their security needs, the Center of Competences in Cybersecurity and Privacy of the University of Porto (C3P), in consortium with the Data Protection Commission (CNPD), Developed a USB stick that according to them returns the privacy control to the user without the user having to worry about the configuration of the applications. The solution consists of a USB stick with a set of software configured to force respect for the privacy of its user. For the development of this tool the PortableApps website was used, an online platform used for distribution of a large variety of portable programs (executable without need to install) open source and available for download. The application developed includes, in addition to other relevant programs, encryption software as well as an encrypted folder on the USB stick that works as a secure folder. Despite the tool consist in a USB data stick, there is always a way to compromise it unless it is set only to read data. Despite its secure use it cannot be considered a viable solution because it is dependable of an operative system and a device with available USB ports.

What is common in most of the OS described above is the use of secure networks that operate as a safe relay to access the internet. Despite the characteristics of the OS, they all have in common the

use of TOR Network of I2P. The I2P network is similar to the TOR network different only in the identity of the outgoing traffic nodes. In TOR, they are randomly and public, in I2P they are held by an identified "someone".

TOR is a network of VPN tunnels over the unsecure web, where user's computers are common routers thereof making workable the entire computer network. Users who only use the TOR browser or another, provided it contains a plugin to allow use of the network, will only be clients of this anonymous network based on .onion domain.

Its operation is quite simple and layered (hence the connection with the analogy of onion). Using a client program (TOR Bundle) previously installed on any user computer, it will act as a proxy, which is a known Internet protocol developed by David Koblas in 1992 (Zwicky et al. 2000) and forward all data packets between client-server.

The I2P is similar to the TOR Network concept of communication layers. The difference is that all nodes in the network are properly identified in a network distributed database. To access all features a fee is applied to the user. The distinguishing element of the TOR Network is precisely the fact that the entire network can be possibly related to someone or some entity.

Each customer has their own I2P router which allows the creation of tunnels for inbound and outbound traffic. A sequence of random two tunnels is created to give way to pass communications between client-server and server-client.

All communications are encrypted point-to-point using an encryption method of four layers composed of a pair of public-key. Data packets are divided by two tunnels and the receiver, which is listening with another set of two tunnels receives data packets for these entries. In the Figure 2, it is possible to observe the secure communication model by pairs of I2P tunnels.

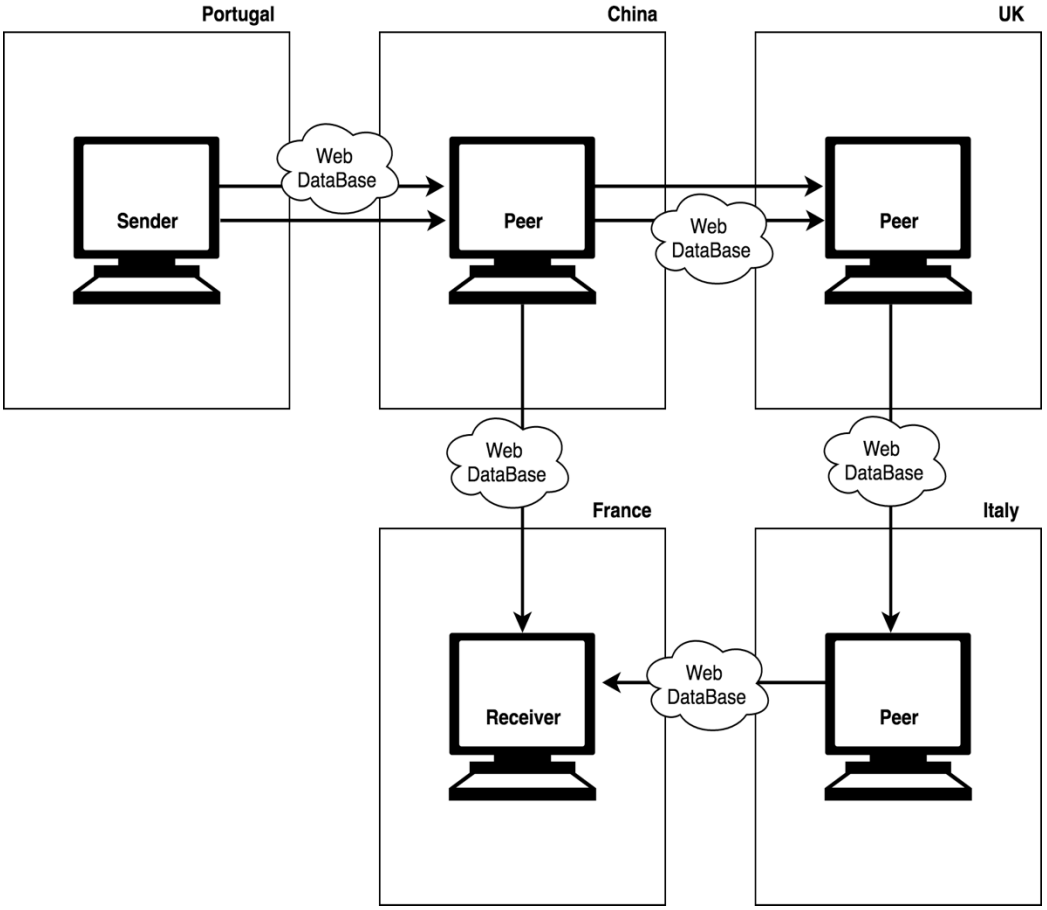

Figure 2- Architecture of I2P routing protocol

4. PROPOSED SOLUTIONS & METHODOLOGY

The objective of this project is to provide security and anonymity to whoever requires a secure operative system. At the end of this doctoral project, a user may create or upgrade a given Linux operative system following specific and scientific approved steps provided by the doctoral work. As an alternative, a given user may just download the concluded prototype. As the objective is to show how can a given user assemble and prepare on its own, a cross platform secure operative systems. This set of actions will traduce itself in a methodology as it achieves the objective.

The proposed solution is applicable in a first stage only to laptops, servers and computer stations, and in a second stage (still under viability study) to Android mobile devices.

In the first stage, a prototype will be concluded as virtual operating system, differing from the options discussed above, such as prevent possible installation on a physical drive, include unique features like MAC Address spoofing, auto update triggers, state of the art cryptography, virtual coin wallet, among other tools, and unique signed kernel. The aim of this prototype is to run from the RAM memory of the computer and in a second stage in a portable mobile device. Most systems nowadays are available to a unique platform.

The methodology (Paranoid operative system methodology for anonymous & secure web browsing) proven effective in the form of the prototype should not require multiple solutions for it practical use, and should not include random production software e.g., LibreOffice. However, users can safely download software from public repositories and install it in the prototype. When to proceed to the shutdown of the prototype, as the methodology implies, all its content will be irretrievably discarded, thus proving its effectiveness.

All systems will operate independently of any hardware serving as host to the virtual environment and will be fully functional in any computer or mobile device. Antagonistically to Windows, that needs to maintain hardware-based architecture to run (Carpenter 2011), the proposed methodology will proof in the form of the prototype that it will operate without limits and with acceptable performance regardless of architecture, virtual machine or mobile device.

In the following image (figure nº. 3) it's presented the conceptual diagram of the prototype in the first stage. According to the preponed methodology there are two possible methods of use, downloaded from a web server or repository for direct use in virtual machine environment, direct use from a portable USB drive unit or CD/DVD.

Requiring at least 1 processing core at 500Mhz and 1GB of RAM as it's possible to oberve, the prototype will connect to the host via 2 ways, directly and through a DVD or USB port, or within a host recurring to a virtual environment, e.g., VirtualBox[8]. With the operative system running it will connect to the web through a proxy sock5 module that pipes all web traffic though it to the TOR network. When using the TOR Browser the user will add an extra layer of anonymity as the browser emulates a new TOR engine that run over the proxy socks5 module. The existing firewall will only accept traffic from the open ports in the proxy socks5 module, thus blocking any other web traffic. This is one unique aspect of the solution when compared with the most current available platforms (please observe table nº.1). If the prototype is being use in a virtual environment the host should have a firewall operating. There will be no need to adjust it, the prototype will use the TOR to go around it. As the TOR consists in a large VPN network without exiting nodes using SSL, the prototype will possess a mechanism that forces the use of HTTPS. If a given web resource cannot comply with this, the user will receive and graphic alert.

[8] VirtualBox - A free and open-source hypervisor for x86 computers

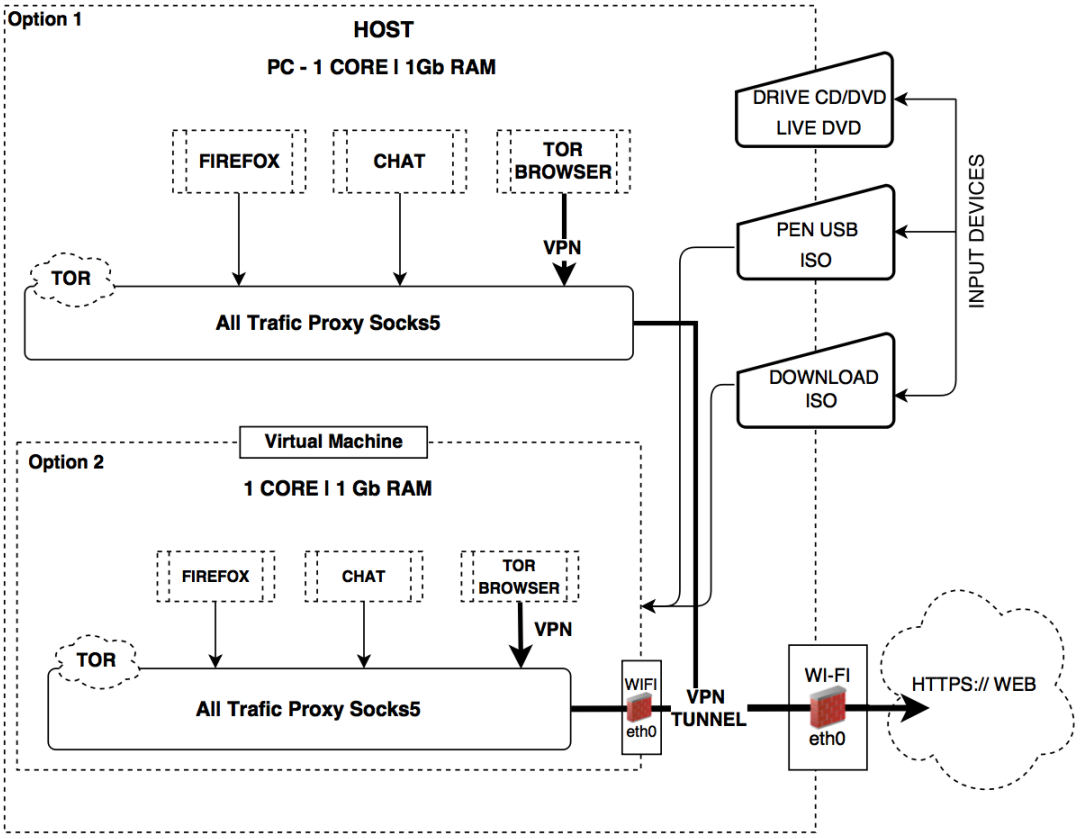

Figure 3 - Conceptual Diagram

4.1. Doctoral Research Method

After exploring the problematic to better comprehend the main challenges and issues, the author proposes to achieve the final objective applying the Investigation-development-action method.

Result of the problematic exploration and methodology design, the prototype is now being developed under a Linux distribution developed and constructed from zero recurring to the Ubuntu 14.04 TLS. This distribution continuously improvement indicated to be the most effective over time, providing the community with hundreds of websites of people discussing Ubuntu's technology and solutions.

The first stage is being developed using the algorithm Linux From Scratch. In a further phase, it will be required to make a comparison of several applications, testing them in a cross reference way. In the second stage of the methodology development, the Cyanogen OS for Mobile Devices will be used to engineer the mobile version of the prototype, thus showing that the methodology is applicable cross platforms.

In both cases, all software of the specific distributions will be removed from the system to be used as source or host, in order to install all necessary software and core configurations like building a signed kernel for the tool.

Early study conducted within the scope of this work point to the need of using the TOR Protocol simultaneously with the I2P. This will to provide extra anonymity ensuring secure protocols that promotes security. This can be achieved by configuring a proxy socks5 module to channel all communications through it and routine it at start-up. After using a secure browser, this will construct a third layer of anonymity and security as three opposite rings of communication, therefore enabling access to the third layer of the deepeweb.

The final stage is to add common communications tools and software. The objective is to test these applications in a challenge sequence way to identify the most effective. This will assure the prototype effectiveness to prevent user's identity and location to be disclosure as the methodology demands.

In the following image (figure nº.4) its observable the prototype tree of content:

Figure 4 - DVD content tree

5. CONCLUSION

The objective is to develop a solid methodology that enables a user to strength or construct a secure operative system distribution. This will be empirically proven in the form of an operative system prototype that enables anonymous & secure web browsing.

This research-in-progress is an elementary phase of the process to design such methodology, overcoming the problematic of online insecurity and capture of private information by hackers or censorship mechanisms. The methodology objective is to create a pattern usable by whom requires it, operating it without the need of specific hardware and following deontological specific aspects. Studies clearly indicate a search for these kind of solutions, and above all, there is a need and constant demand for it in Portugal where it may currently (05-2017) be of origin, the unique one.

The future work is the inclusion of the prototype's components. Having already concluded the security testing of all components, connecting them in one environment without interferences between them is the objective for this point. At the end of this stage the prototype will be targeted with viruses, Trojan horses, root kits, firewalls and other security vulnerability or constrainer program to verify if effectiveness and all traffic emerging from it will be snifered to observe possible breaches in security.

All the research will be conducted with the most rigorous techniques and scientific methodologies, peer reviewed by PhD professors in the field of computer sciences and information security, assuring a scientific approach, as opposite to the alternatives similarly available in the market with an unknown development cycle, agenda or origin.

Currently, the scientific methodology implied is exploration-action-development. Others might be used.

REFERENCES

Assange J. (2013). "The spy files": https://twitter.com/wikileaks/status/342812446534283264

Barcena M., Wueest C. (2015). "Insecurity of the internet of things," Symantec, Tech. Report: https://www.symantec.com/content/dam/symantec/docs/white-papers/insecurity-in-the-internet-of-things-en.pdf

Bessa P. (2015). "Dados dos utilizadores do euromilhões.com roubados": http://pplware.sapo.pt/informacao/alerta-dados-dosutilizadores-do-euromilhoes-com-roubados

Boavida F., Bernardes M., Vapi P. (2013). Administração de Redes Informáticas, FCA.

Carpenter T. (2011). Microsoft Windows Operating System Essentials, 1st ed., John Wiley and Sons.

Coelho N. (2017) Vodafone security bulletin for ransomware WannaCry. Vodafone Portugal Internal Bulletin.

Deibert R., Palfrey J., Rohozinski R., Zittrain J., Stein J. G. (2008). Access Denied: The Practice and Policy of Global Internet Filtering, MIT Press.

Kuruvilla S., Lee C., Gallagher M. (2011). From Iron Rice Bowl to Informalization: Markets, Workers, and the State in a Changing China, 1st ed, Cornell University Press.

Locati F. (2015). OpenStack Cloud Security, Packt Publishing Ltd.

Lopez J., Ray I., Crispo B. (2015). Risks and Security of Internet and Systems: 9th International Conference, CRiSIS 2014, Trento, Italy, Revised Selected Papers, Springer.

Moore R. (2014). Cybercrime: Investigating High-Technology Computer Crime, Routledge.

Murugesan S. (2009). Handbook of Research on Web 2.0, 3.0, and X.0., 1st ed., Information Science Reference.

O'Day P. (2013). NSA Surveillance: How it's happening and why you should care, Pacific University of Oregon.

O'Reilly T. (2009). What is Web 2.0, 1st ed., O'Reilly Media Inc.

Raymond E. (1996). New Hacker's Dictionary, MIT Press.

Santos P., Bessa R., Pimentel C. (2008). CyberWar – O Fenómeno, as tecnologias e os atores, 1st ed., FCA.

Shea B. (2002). Have You Locked the Castle Gate, 1st ed., Addison-Wesley Professional.

Shelly G. B., Campbell J. (2014). Discovering the Internet: Complete, 5th ed., Cengage Learning.

Stats I. L. (2015). Data referent to internet usage in 2015: http://www.Internetlivestats.com/watch/Internet-users.

Walker H. (2009). Ed., Improving Internet Access to Help Small Business Compete in a Global Economy, 1st ed., Nova Science Publishers.

Zwicky E., Cooper S., Chapman B. (2000). Building Internet Firewalls, 1st ed., O'Reilly Media Inc.

Zúquete A. (2014). Segurança em Redes Informáticas, FCA.