Chapter 23
POSMASWEB:
Paranoid Operating System Methodology for Anonymous and Secure Web Browsing

Nuno Ricardo Mateus-Coelho
https://orcid.org/0000-0001-5517-9181
Universidade de Trás-os-Montes e Alto Douro, Portugal

Benjamim Ribeiro Fonseca
Universidade de Trás-os-Montes e Alto Douro, Portugal

António Vieira Castro
Instituto Superior de Engenharia do Porto, Portugal

ABSTRACT

It has recently been discovered that large companies and nations "observe" their customers and citizens, disregarding any remaining moral and technological lines, being able to listen to telephone conversations and monitoring communications through powerful monitoring and surveillance programs. Elsewhere on the planet, nations in turmoil or wrapped in a cloak of censorship persecute their citizens, controlling them by denying them access to the free web without the threat of repercussions that threatens their dignity. To support the present research, an analysis of platforms that allow anonymous and secure browsing and a study of technologies and programs with potential privacy breach and computer intrusion were performed. The main objective of this work was to analyse the computer monitoring and surveillance technologies, identifying the available tools, trying to find potential solutions, developing and providing a methodology that enhances any desktop, server, or mobile operating system, with characteristics that combat the exposed in this summary.

DOI: 10.4018/978-1-7998-5728-0.ch023

Copyright © 2021, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

INTRODUCTION

According to David Whitley (Whitley, 2009) human communication goes back to the earliest history records, approximately thirty to forty thousand years ago. Initially, they were symbols used for the passage of knowledge, e.g., to identify behaviours or mundane aspects to the surroundings and territories, dangers or just leisure. It was about 9.000 years ago that man began the arduous task of writing words with meaning and with the intention of passing or retaining knowledge the future generations. The organized writing system with semantic content also appeared approximately 6.000 years ago. From then onwards, the great technological evolutions that followed were always accompanied by the registration of activities and their planning, in written form in every means possible (Whitley, 2009). The evolution was such that, nowadays, writing is mostly done digitally by means of multimedia tools and data entry in computers, being atomically spread by technological means by millions and millions of people across continents. According to Mark Zuckerberg (Zuckerberg, 2015), in 2015, on 8 September, 1 in 7 humans were linked at the same time to Facebook (digital social network) and more was to be expected in the future, aiming to double that amount by the end of 2020, an astronomical deed from the time the man made engravings in cave walls.

We live in a time when society is challenged by sudden change with social, political, economic and high environmental costs. This volatility implies strong consequences for the (in) security of societies and organizations. The speed at which events happen, new technological offers, new trends, products, problems and solutions rises, create a disruption that already has today, and despite the efforts of those who regulate, an impact virtually impossible to contain or hide. The research and massive use of information and social sharing of it, was created by the advent Web 2.0 or 2nd generation Web, 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, 2010), (Priya et al., 2019), created an unique digital phenomena, comparable only to the human ecological footprint. The digital footprint implies that everything that is shared and exposed on the Web, to be stored somewhere in it, allowing third parties to access and save this information in computational clusters with estimated useful life impossible to calculate, thus being accessible to others for many, many generations.

By relying on Cloud platforms (data storage in virtualized computing environments) and publishing personal information on social networks, individuals opened the door to cybercrime (crimes committed using information technologies) which for years targeted only corporations. Being a living entity, in the broadest sense of the sentence, globalization, this network made up of people and machines, is also a source of misinformation directed to nations that compete with each other, where, whom first holds the validated information has in fact, leadership (Zarghoon et al., 2017), and to achieve this, whether economic or strategic, mechanisms are created that advocate computer insecurity through violation, decoding, modification and interception of data with the objective of retaining private information for their own benefit.

Computer security is constantly being tested. According to Paulo Santos (Santos et al., 2008) from computer pirates commonly known as hackers to government intelligence agencies, everyone wants a piece of this *El Dorado*, being just a matter of ego or economic benefits and strategic advantage in the game of international politics. Also, computer systems connected using a network and, above all, the wide network that is the Web, are daily used to store and manipulate information by millions of people and organizations. According to Herman Walker (Walker, 2009) schools, universities, medical offices, students, teachers, medical staff or any indigent, all of them exchange information through computer

30 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/posmasweb/261743

Related Content

Security Issues and Solutions for Resource-Constrained IoT Applications Using Lightweight Cryptography
Kamalendu Pal (2023). *Cybersecurity Issues, Challenges, and Solutions in the Business World (pp. 138-159).*
www.irma-international.org/chapter/security-issues-and-solutions-for-resource-constrained-iot-applications-using-lightweight-cryptography/313864

Prevention of Cyber Crime in Cybercafés
Ogochukwu Thaddaeus Emiri (2008). *Security and Software for Cybercafes (pp. 239-252).*
www.irma-international.org/chapter/prevention-cyber-crime-cybercafés/28540

Metamorphic malware detection using opcode frequency rate and decision tree
Mahmood Fazlali, Peyman Khodamoradi, Farhad Mardukhi, Masoud Nosratiand Mohammad Mahdi Dehshibi (2016). *International Journal of Information Security and Privacy (pp. 67-86).*
www.irma-international.org/article/metamorphic-malware-detection-using-opcode-frequency-rate-and-decision-tree/160775

Moral Rights in the Australian Public Sector
Lynley Hocking (2007). *Encyclopedia of Information Ethics and Security (pp. 470-477).*
www.irma-international.org/chapter/moral-rights-australian-public-sector/13514

CSMCSM: Client-Server Model for Comprehensive Security in MANETs
Hatem Mahmoud Salama, Mohamed Zaki Abd El Mageed, Gouda Ismail Mohamed Salamaand Khaled Mahmoud Badran (2021). *International Journal of Information Security and Privacy (pp. 44-64).*
www.irma-international.org/article/csmcsm/273591