EDITORIAL

Edition 2, Volume 2, December 2022

ARIS^2 - Advanced Research on Information Systems Security

an International Journal

Nuno Mateus-Coelho, PhD *

1. INTRODUCTION

The globe continues to support an abnormal occurrence that has a severe influence on cyber security, which is the conflict between Russia and Ukraine that persists in establishing the first cyber war. This assistance comes as the year 2022 reaches its last range. Since the beginning of this fight, two enormous organizations have been formed in order to investigate potential weaknesses in the security measures used by either side. They exploit weaknesses, resort to force, or engage in social engineering in order to achieve their goals. The protection of information, actors, and the frameworks within which they operate has become an extremely important battle, and science plays a significant part in both the performance and maintenance of security actors in this situation.

Two out of ten research papers that were submitted to ARIS2 - Advanced Research on Information Systems Security, an International Journal were chosen to be published in the first regular issue of 2022. This resulted in an acceptance rate of twenty percent for the journal. These two papers demonstrate that information security, awareness, and resilient systems are fundamental components of modern information systems. Furthermore, modern information systems now have the additional responsibility, in particular and above all to maintain the confidentiality of user-provided private information. According to research that was conducted by members of the industry, common enterprises are not only the targets of cyber assaults, but they are also being compelled on a vast scale by ransomware blackmail and extortion [1].

* Editor-in-chief of ARIS^2, Portugal. E-mail: nuno.coelho@ulusofona.pt

Before making their products available to the general public, businesses need to take into account the new dangers and issues that have arisen as a result of the widespread utilization of resources that enable quick connectivity, such as the smartphone. This allows for the anticipation of potential vulnerabilities and the reduction of risk [2].

Academic study has emerged at this particular moment with consistent solutions that have to be communicated to the public as the path that ought to be taken in the form of scientific investigation [3].

Moreover, according to studies that were conducted not too long ago, the field of study into information security is developing, although growth is neither simple nor linear [4]. Research indicates that every time there is an improvement in security, a new zero-day vulnerability or loophole is created, yet the media overlooks these breakthroughs. After a long length of time spent working discreetly, Zero-Day has the potential to have an influence not just on businesses but also on individuals in general [5]. Through study and investigation that often makes use of methodologies such as forensics and threat analysis, societies are able to anticipate the repercussions of a zero-day vulnerability, which ultimately results in a more secure use of technology [6].

2. STRUCTURE

In the second issue of the ARIS^2 - Journal, the reader will have *online* access to seven research works as follows:

1. Post-Quantum Cryptography Challenges.
2. (In)Security in Wi-Fi networks: a systematic review.
3. Can machine learning be used to detect malware? Android OS Case Study.
4. Steganography and Computer Forensics - the art of hiding information: a systematic review.
5. Web 3.0 and Cybersecurity – Short Paper.
6. Predicting Cybersecurity Risk - A Methodology for Assessments.
7. Case study to identify vulnerabilities in applications developed for the Android platform.
8. Cybersecurity Threats for a Web Development.

The papers evaluated by double blind review system belong to authors who presented the results of their studies that fit in the scientific areas of the ARIS^2 Journal; so, they were accepted for publication in this international scientific journal.

3. ACKNOLEDGEMENTS

We would like to thank the authors who have submitted their manuscripts and all the reviewers for their valuable contributions. The scientific importance of the publications in this Issue of the ARIS² - Journal is a strong reason for other authors to submit works for future Regular and Special Issues.

REFERENCES

[1] M. M. Cruz-Cunha and N. R. Mateus-Coelho, *Handbook of Research on Cyber Crime and Information Privacy*. IGI Global, 2021. DOI: 10.4018/978-1-7998-5728-0

[2] N. Coelho, B. Fonseca, and A. Castro, "Paranoid operative system methodology for Anonymous & Secure Web Browsing, doctoral project," *Atas da 17ª Conferência da Associação Portuguesa de Sistemas de Informação*, 2017. DOI: 10.18803/capsi.v17.127-143

[3] N. Mateus-Coelho and M. Cruz-Cunha, "Serverless Service Architectures and Security Minimals," *2022 10th International Symposium on Digital Forensics and Security (ISDFS)*, 2022, pp. 1-6, doi: 10.1109/ISDFS55398.2022.9800779.

[4] N. Mateus-Coelho, "A new methodology for the development of secure and Paranoid Operating Systems," *Procedia Computer Science*, vol. 181, pp. 1207–1215, 2021. DOI: 10.1016/j.procs.2021.01.318

[5] M. Saraiva and N. Coelho, "CyberSoc Implementation Plan," *2022 10th International Symposium on Digital Forensics and Security (ISDFS)*, 2022, pp. 1-6, doi: 10.1109/ISDFS55398.2022.9800819.

[6] F. Alves, N. Mateus-Coelho and M. Cruz-Cunha, "ChevroCrypto – Security & Cryptography Broker," *2022 10th International Symposium on Digital Forensics and Security (ISDFS)*, 2022, pp. 1-5, doi: 10.1109/ISDFS55398.2022.9800797.

How to cite this article:

Mateus-Coelho, N. (2022*). The Editorial of ARIS2 - Advanced Research on Information Systems Security, an International Journal*, Vol. 2, No. 2, 1-3.