CYBERSECURITY ASSESSMENT AND CERTIFICATION OF CRITICAL INFRASTRUCTURES

Ioana Corina BOGDAN[1], Emil SIMION[2]

Cybersecurity is a field that unifies concepts from various fundamental areas: mathematics, physics, computer science, electronics, sociology, and management. This field is challenging for government authorities, academic institutions, and private entities alike. By pooling the resources of these three actors, we can build secure and resilient systems. In this context, several challenges emerge, such as the exchange of knowledge and expertise, collaborative research projects, the organization of internships and scholarship programs, the exchange of threat intelligence, training, and awareness, and finally, the standardization and regulatory component. The evolving nature of cyber threats and the growing sophistication of attackers necessitate robust and adaptable security frameworks. A "defense-in-depth security model" is mandatory in this context as it offers multiple layers of protection, ensuring that if one defense mechanism fails, others remain in place to prevent breaches. In this paper, we propose a defense-in-depth security model and highlight how key points within the model can be interconnected.

Keywords: Cryptographic algorithms and protocols, Cryptographic module evaluation ISO19790, Common Criteria ISO1540

1. Introduction

In our days, according to U.S. military doctrine, threats arise from five major areas: terrestrial threats (earthquakes, volcanic eruption, etc.), maritime/fluvial threats (floods, tsunamis, coastal erosion, etc.), space threats (meteorite falls, electromagnetic pulses, satellite hijacking or jamming), airborne threats (aerial attacks biological warfare, pollution, etc.), and cyber threats (malware, zero-days, phishing, APT, etc.). The fundamental difference between these areas is that the latter one is induced by human factors, meanwhile the first four threats are governed by the nature laws, [1]-[3]. For this reason, our society conducts its activities in two strongly interconnected spaces: the physical, and the virtual space, respectively. While we have identified and mitigated threats in the

[1] Assistant professor, Faculty of Electrical Engineering and Computer Science, Department of Electronics and Computers, “Transilvania” University of Brasov & CiTi, Brasov, Romania, e-mail: corina.bogdan@unitbv.ro

[2] Associate professor, Department of Mathematical Methods and Models, National University of Science and Technology POLITEHNICA Bucharest & CiTi, Bucharest, Romania, e-mail: emil.simion@upb.ro

physical world, we cannot say the same thing for the virtual space. The internet environment has been publicly available for approximately 30 years. All vital elements for the proper functioning of society (electricity networks, drinking water systems, healthcare, transportation systems, banking systems, e-governance systems, media, etc.) are secured through cyber means, [1]-[2]. On the other hand, threat agents come from three major areas: lone hackers, cybercrime groups, and state actors, [4]. These entities have diverse motivations: financial, extremist-ideological, and strategic, respectively.

Cyber threats are generated by several factors, [1]-[2]:

- the vulnerabilities existence from the point of view of technology, procedure, and human beings manifested at the network and information systems level,
- the availability and accessibility of hacking resources,
- low levels cybersecurity awareness and hygiene in the cyber space,
- the insufficient training and specialization in the field of cybersecurity, both among professionals and managers,
- the regulatory and procedural gaps,
- the expansion of the range of devices,
- the lack of regulatory framework and policies for managing cyber risks in the supply chain.

In Figure 1, a defense-in-depth security model is presented. The first security element is represented by security algorithms and protocols. These are mathematical elements materialized through implementation in the second element, cryptographic modules (which can be hardware or software). The latter are integrated into security products that are used to protect informational systems. On each defense layer, various techniques and standards are applied. These are discussed in the next section of the paper. In other words, we mentioned some of the multiple skills, enumerating the advanced knowledge of cryptography, security risk management, networking and systems knowledge, ethical hacking and familiarity with security technologies, communication efficiency (given by diverse teams that need to interact with technical, management, and end users), incident management, programming, analysis, and critical thinking.

In the authors' view, the main characteristic of the article is that it achieves an integrated approach to the various evaluation rings of the information protection system: algorithms, cryptographic modules, security products, and information security management. Given the rapid pace of technological evolution (AI and quantum computing), the need for an initiative-taking approach to adapt and continuously improve security systems is emphasized. This is essential to address new threats and challenges that may arise in the context of technological changes.

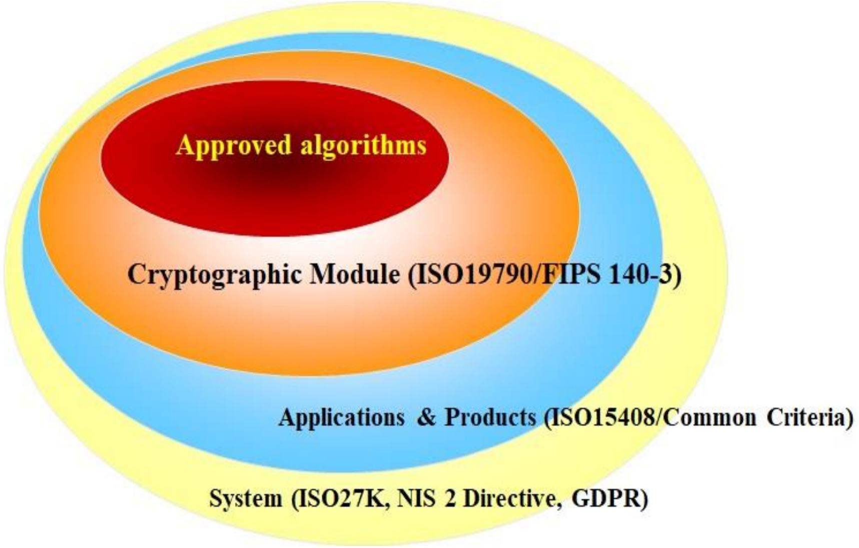
Approved algorithms
Cryptographic Module (ISO19790/FIPS 140-3)
Applications & Products (ISO15408/Common Criteria)
System (ISO27K, NIS 2 Directive, GDPR)

Fig. 1 The model for security layers.

This paper is divided into five parts. In Section 2, we present a universal technique for statistical evaluation of cryptographic algorithms and protocols, particularly focusing on how statistical tests [5]-[7] are employed to statistically validate encryption algorithms (including block or stream), and random number generators used in cryptographic applications. After presenting the cryptographic algorithms security from the point of view testing and demonstration, the next step is building the cryptographic module which could be a hardware device or a software component, such as a cryptographic library. In Section 3, we present the requirements of the ISO 19790 reference standard [8], which is equivalent to the FIPS 140-3 standard. ISO standards can be applied by the entire developer community, while FIPS standards, issued by the federal government, are mandatory for them. The evaluation of applications and products are discussed in Section 4 using the ISO 15408 standard [9]-[11], also known as the Common Criteria. Finally, before presenting the conclusion and analysis results of this paper, we discuss in section 5 several challenges related to the security evaluation in connection with modern technologies and the dynamics of our society.

Each chapter of the paper addresses an essential aspect of cybersecurity, having utility both in practice and research:

a) theoretical foundations of statistical evaluation of cryptographic algorithms: This chapter explores the basic principles and techniques used in assessing cryptographic statistical performance.
b) evaluation of cryptographic modules: The analysis and certification of cryptographic modules are essential for ensuring the integrity and confidentiality of information.

c) application evaluation: This chapter focuses on the implementation of cryptographic solutions in various practical applications.
d) system evaluation: The integration of security measures in complex systems is crucial for effective protection against cyber threats.

The paper explores how these components interact and support each other, which is not always considered in previous works. By analyzing the synergies among them, we aim to contribute to the development of more effective frameworks for cybersecurity.

Overall, connecting these four components allows for an integrated understanding of the challenges and solutions in the field of cybersecurity. This interconnected approach not only helps practitioners build robust security frameworks but also opens new avenues for research, fostering advancements in the field.

2. Statistical evaluation of cryptographic algorithms

Statistical tests are used in cryptography and contribute to the evaluation and validation of cryptographic algorithms and protocols. A series of applications of statistical tests are in the field of assessing the statistical behavior of random number generators, analyzing the resilience of algorithms against various types of attacks, validating cryptographic protocols, and detecting anomalies in the behavior of cryptographic systems—factors that may indicate a potential security breach or vulnerability in implementation.

2.1 Brief Presentation of the Concept of a Statistical Test

A general technique for evaluating cryptographic algorithms is based on statistical tests. The procedure is the following: samples are built using clear text inputs and strongly (auto)correlated keys. If these samples deviate from randomness, then the evaluated algorithm does not meet the requirements for this criterion.

The statistical test operates with the concept of a sample, based on which, with a certain margin of error, it decides on a statistical hypothesis. To clarify the ideas, we will define the following concepts: sample, statistical hypothesis, and statistical test.

Sample: Corresponds to a representative subset of a larger population, which is selected with well-defined properties to provide quantitative information about the population. The sample is a part of the population studied and analyzed in the context of research or an experiment. The objective of using a sample is to make valid inferences or generalizations about the entire population based on the information obtained from the subset.

Statistical Hypothesis: It represents a statement or assumption formulated to be evaluated in a study or statistical research. There are two main types of statistical hypotheses, namely null and alternative hypotheses, respectively. The null hypothesis (H_0) corresponds to a statement asserting that there is no significant difference, no relationship, or no effect in the population or in a dataset. The alternative hypothesis (H_A) is opposite to the null hypothesis and suggests that there is a significant difference in the studied dataset.

Statistical Test: It is a mathematical statistical procedure used to make inferences or test hypotheses about the characteristics of a population, based on information obtained from a representative sample of it. The purpose of statistical tests is to assess whether the observed differences or associations in the sample are significant and can be generalized to the entire population.

As mentioned above, the process of statistical testing is subject to errors. To solidify the ideas, let's assume that we are trying to distinguish between two statistical hypotheses: H0, the null hypothesis, and H1, the alternative hypothesis. Two types of errors could be encountered:

a) First type error, also known as the level of significance, i.e. the probability of rejecting the null hypothesis when it is true: α=Pr(reject H_0| H_0 is true);

b) Second type error, which represents the probability of failing to reject the null hypothesis when it is false: β=Pr(accept H_0|H_0 is false), the complementary value of β is denoted as the test's power: 1-β=Pr(reject H_0|H_0 is false).

It is not possible to simultaneously minimize both errors, α and β, as the reduction of α leads to an increase in β, and vice versa. To address this challenge, one approach is to control the value of α while calculating the probability of β.

2.2 NIST SP 800-22 Statistical Test Suite

The NIST SP 800-22 Statistical Test Suite is described as a collection of statistical tests used to assess the quality and robustness of random number generators and cryptographic algorithms. The Statistical Test is developed by the National Institute of Standards and Technology (NIST) with the aim of providing evaluation tools for assessing the performance of encryption systems and other cryptographic applications. The test suite includes a few series of statistical tests focusing on evaluating specific features of generated bit sequences, such as uniformity, independence, etc. Each of these tests were designed to identify irregularities or deviations from the expected behavior of a random number generator or cryptographic algorithm. Proper implementation of these tests helps to ensure that cryptographic algorithms and protocols are resistant to attacks and provide adequate security. Regarding the NIST SP 800-22 test suite, this one contains a total of 15 statistical tests that can be classified, in terms of reference distributions, into three classes: χ^2 (chi-squared), normal, and half-normal.

Table 1

Reference distribution of NIST SP 800-22 statistical test suite

Test	Reference Distribution
Frequency Test within a Block	χ^2(N)
Test for the Longest Run of Ones in a Block	χ^2(K)
Binary Matrix Rank Test	χ^2 (2)
Non-overlapping Template Matching Test	χ^2 (N)
Overlapping Template Matching Test	χ^2 (K)
Linear Complexity Test	χ^2 (K)
Serial Test	χ^2 (2^{m-1})+ χ^2 (2^{m-2})
Approximate Entropy Test	χ^2 (2^m)
Random Excursions Test	χ^2 (5)
Runs Test	normal
Discrete Fourier Transform (Spectral) Test	normal
Maurer’s “Universal Statistical” Test	normal
Cumulative Sums (Cusum) Test	normal
Frequency (monobit) test	half normal

A binary sequence may pass or fail a particular type of test. Hence, natural questions arise: how do we integrate the results of the fifteen statistical tests? How can a classification be made based on their strength, implementation complexity, the minimum sample size to ensure a first-order error probability, and the independence of tests? To answer these questions, it is essential to develop a systematic approach that considers each test's characteristics and their interdependence. For instance, combining results from multiple tests requires careful evaluation of test reliability, and adjustments to sample size may be necessary depending on the desired error thresholds. The integration process may also involve weighing each test’s complexity and computational demands to determine the most efficient approach for a given context.

These statistical tests can be utilized in the following contexts:

a) evaluation of random number generators by assessing the quality and randomness of sequences generated by noise generators.

b) evaluation of block or stream cryptographic algorithms by testing and verifying the robustness and randomness properties of cryptographic algorithms, whether they are block ciphers or stream ciphers.

The integration of test results involves considering the outcomes of each individual test and understanding their collective implications. The classification of tests based on their strengths, implementation complexity, and other factors can aid in selecting appropriate tests for specific applications. The minimum sample size necessary to ensure a certain level of error probability and the independence of the tests are crucial considerations in the effective application of these statistical tests.

2.3 Test Construction

Statistical tests are built following the law of large numbers [12-13]. This theorem can be formulated in two ways:

Theorem 1 (Lyapunov). *If (g_n) is a series of independent random variables which shares the same distribution of mean m and variance □, then as n becomes sufficiently large, the following holds true:*

$$Pr(u < g_1 + \ldots + g_n < v) \approx \Phi\left(\frac{v - n \cdot m + \frac{1}{2}}{\sigma\sqrt{n}}\right) - \Phi\left(\frac{u - n \cdot m - \frac{1}{2}}{\sigma\sqrt{n}}\right).$$

Theorem 2 (De Moivre) *If (g_n) is a series of binary independent random variables with Pr(X=1)=p and Pr(X=0)=q, then as n becomes sufficiently large, the following holds true:*

$$Pr(u < g_1 + \ldots + g_n < v) \approx \Phi\left(\frac{v - n \cdot p + \frac{1}{2}}{\sigma\sqrt{npq}}\right) - \Phi\left(\frac{u - n \cdot p - \frac{1}{2}}{\sigma\sqrt{npq}}\right).$$

A fundamental question is related to the minimum sample size such that the relative frequency approximates the probability with an error ε > 0, and this approximation is valid with a confidence level of 1-α. Mathematically, this is rewritten as:

$$Pr(\,|\nu_n - p| < \varepsilon) \geq 1 - \alpha,$$

where $\nu_n = \frac{g_1 + \ldots + g_n}{n}$, representing the sequence of relative occurrence of the symbol 1.

Using the *Theorem 2*, we determine the minimum sample size required to attain, with error ε>0, the rejection rate α:

$$n_{min} = \left[\frac{1}{4\varepsilon^2} u^2_{1-\frac{\alpha}{2}}\right]$$

where $u^2{}_{1\text{-}\alpha/2}$ is the quantile of order 1-α/2 of the normal distribution.

An unresolved issue is the problem of the independence of statistical tests as well as the order of their execution based on their implementation complexity.

2.4 Sample Construction

Samples are developed from sources of low entropy which allow for clearer identification of weaknesses in the generation of random sequences by a system, facilitating the detection of deviations from the ideal value of randomness. By using low-entropy sources, we can better understand the limits and constraints of the tests, ensuring that any random number generator can pass under more controlled and predictable conditions. Furthermore, this approach can help simulate worst-case scenarios, which are useful for validating the robustness and sensitivity of statistical tests used in cryptographic applications or other fields that rely on randomness. For example, in the testing of cryptographic algorithm candidates for AES, the following samples were used: 128-Bit Key Avalanche, Plaintext Avalanche, Plaintext/Ciphertext Correlation, Cipher Block Chaining Mode, Random Plaintext/Random 128-Bit Keys, Low Density Plaintext, Low Density 128-Bit Keys, High Density Plaintext, High Density 128-Bit Keys.

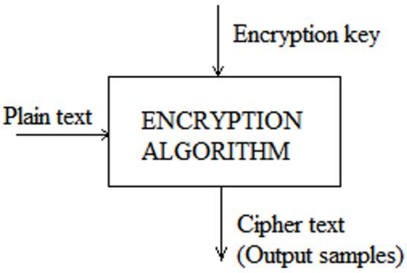

Fig. 2. Sample construction.

3. Cryptographic Module Evaluation

In the following, we will provide a brief description for each evaluation domain of cryptographic module, highlighting their importance and relevance to the security of cryptographic modules. This will help establish a clear connection between the evaluation criteria and the practical implications for cybersecurity. The evaluation of cryptographic modules is conducted using the FIPS 140-3 standard [14], whose ISO equivalent is ISO 19790. Within this standard, eleven evaluation domains are specified:

1) Documentation of the cryptographic module. Based on the specification of the algorithms used, the description of the cryptographic module architecture (considering the module structure, its interfaces, data flows, and memory map) is taken into consideration.
2) Ports and interfaces of the cryptographic module. The physical or logical entry and exit points of clear data, management, and encrypted data within the cryptographic module need to be described. Interfaces are sets of rules and protocols that govern the communication and interaction between the

cryptographic module and other components of the system. They define how data is transmitted and received, as well as how the components interact with each other.

3) Roles, services, and authentication. A cryptographic module can have multiple roles: administrator, user, or system. Each role may have access to one or more services, including configuration and management, encryption, decryption, key generation, and electronic signing. Access is granted through the authentication process, which can be achieved using multifactor techniques and methods (such as username and password, physical token, biometric properties, etc.).
4) Finite state machine (FSM) model. The FSM is a paradigm used in designing and describing the behavior of systems, where the system can exist in a finite number of distinct states. A cryptographic FSM can transition between these states in response to specific events or inputs, in a very precis manner. The finite state machine model is useful in demonstrating the reliability and robustness of the cryptographic product.
5) Operating environment. The operational environment of a cryptographic module refers to the management of the necessary software, firmware, and/or hardware components for the cryptographic module to operate. The operational environment can be non-modifiable, such as firmware included in ROM, or software included in a computer with I/O (input/output) devices disabled. Additionally, it can be modifiable, for example, firmware included in RAM or software executed by a general-purpose computer.
6) Physical security. Physical attacks (whether invasive or not) on a cryptographic module, aimed at extracting critical security parameters such as encryption and/or authentication keys or algorithms. To prevent such invasive attacks, measures such as tamper resistance (special screws), tamper evidence (security seals), and tamper detection (sensors to detect changes in security conditions) and tamper response (actions leading to zeroizing critical security parameters and logging these events) can be imposed.
7) Electromagnetic compatibility. It refers to the cryptographic module's ability to operate properly in the presence of other electronic devices without causing unwanted electromagnetic interference and without being affected by such external interferences. In practice, the cryptographic module must adhere to specific emission limits to avoid interference with other network equipment.
8) Key management. The security requirements for cryptographic key management cover the entire lifecycle of cryptographic keys (generation, pre-activation, operation, storage, destruction), cryptographic key components, and critical security parameters used by the cryptographic module. All these aspects must be included and detailed within the documentation. This field covers both the generation of random numbers and the generation of secret keys, ephemeral keys, as well as pairs of public and private keys. It is

important to note the distinction between secret keys specific to symmetric systems and private keys specific to asymmetric systems.

9) Cryptographic module self-tests. In this area we focus on to the ability of a cryptographic module to perform automated tests or self-testing to assess and confirm the correct functionality of its own components and cryptographic operations.
10) The design assurance process involves the careful assessment and validation of each stage of the project, including requirement specification, architectural design, implementation, testing, and, if applicable, certification according to relevant security standards or regulations., and
11) Mitigation of other attacks (such as TEMPEST, attacks in the implementation environment or DDoS).

The evaluation of the above-mentioned domains may require the use of specific hardware testing platforms or tools, such as oscilloscopes, development boards, etc. As a result of the evaluation process, the cryptographic module obtains a confidence level ranging from 1 to 4, with level 4 being the highest.

It should be noted that the evaluation process is continuous, with the development of innovative technologies such as artificial intelligence and quantum computing bringing forth new categories of attacks.

4. Application Evaluation

The Common Criteria or ISO 15408 is an internationally recognized standard for the evaluation and certification of information technology products and systems, including the cybersecurity component. It provides a common framework for assessing the security of IT products, enabling users to compare and evaluate security products from a wide range of vendors.

On the Common Criteria website users can access relevant documentation such as technical specifications, evaluation and certification guides, and other resources to help them understand and implement the Common Criteria standard. The website is managed by the International Organization for Standardization (ISO) and is available in multiple languages.

The Common Criteria (CC) evaluation process is a standardized methodology for assessing the security of information systems and hardware and software products and is structured following a number of stages, as given below:

1) Evaluation Planning: This is the first step in the evaluation process, where the evaluation's purpose is established, and planning takes place. This stage includes defining objectives, identifying security requirements, and determining the required assurance level. Also in this phase we need to consider the available technical and human resources.
2) Security Specifications Development: In this stage, security specifications are developed to define the security requirements of the evaluated product. These specifications are described in a document called the "Security Target" (ST).

3) Design Evaluation: This stage involves assessing design plans and associated documents, as well as the security requirements established in the ST. Design evaluation may also include reviewing design specifications and other documents.
4) Product-Level Evaluation: In this stage, the product is tested and evaluated against the security specifications outlined in the ST. This stage may include security testing, source code analysis, and technical inspection.
5) Supplementary Evaluation: This stage may be used to assess specific aspects of the product not covered in the product-level evaluation. For example, it can be used to evaluate how the product integrates with other products or to assess the product's performance under stress conditions.
6) Certification and Approval: Upon completion of the evaluation, a certification agency may issue a certificate for the evaluated product, attesting that the product meets the security requirements established in the ST. Ultimately, the product is approved for use in accordance with the defined security requirements.

The evaluation standard is divided into three parts. Part 1 presents the overall model and the concepts underlying the standard.

The standard classifies, in the first part, evaluated products into 7 levels of evaluation assurance level (EAL) as follows:

EAL1/ Functional testing: Functional evaluation of the product or system, with verification of documentation and implementation.

EAL2/ Structural testing: Functional evaluation of the product or system, with verification of documentation, implementation, and an analysis of known vulnerabilities.

EAL3/ Methodically tested and checked: Functional evaluation of the product or system, with verification of documentation, implementation, an analysis of known vulnerabilities, and an extended security test.

EAL4/ Methodically designed, tested, and reviewed: Functional evaluation of the product or system, with verification of documentation, implementation, an analysis of known vulnerabilities, and an extended security test conducted by independent evaluators.

EAL5/ Semi-formally designed and tested: Functional evaluation of the product or system, with verification of documentation, implementation, an analysis of known vulnerabilities, and an extended security test conducted by independent evaluators, along with security testing in production environments.

EAL6/ Semi-formally verified design and tested: Functional evaluation of the product or system, with verification of documentation, implementation, an analysis of known vulnerabilities, and an extended security test conducted by independent evaluators. It includes security testing in production environments and evaluation against specific threats.

EAL7/ Formally verified design and tested: Functional evaluation of the product or system, with verification of documentation, implementation, an analysis of known vulnerabilities, and an extended security test conducted by independent evaluators. It includes security testing in production environments, and evaluation against sophisticated and persistent threats.

The costs of evaluation are quantified in financial resources and time allocated to the process. In today's demanding environment, driven by a rush to operationalize information infrastructures, developers omit certain stages of the evaluation process. Most developers prefer to deploy the product with functional testing, intending to address any malfunctions that may arise after deployment. The eleven security functional requirements are described in Part 2. These are structured into eleven classes, families, and components. Classes represent the broad categories of security functionality. They define broad domains of functionality or security objectives. Families represent more specific groups of security objectives, framed within the context of classes. They provide additional details about security objectives. Components are the most detailed level of the structure and provide specific requirements for achieving the security objectives established in the respective families. For example, a class could be "Access Control," within which a family might be "Authentication" or "Authorization." Within the "Authentication" family, a component could specify detailed requirements for the authentication process, such as password management or the use of cryptographic keys. Part 3 of the standards is focused on security assurance requirements: 1) development (architectural design, functional specification, design of toe, implementation representation, target security functions internals, security policy modeling), 2) guidance development (operational user guidance, preparative user guidance), 3) life cycle (life cycle definition, configuration management scope and capabilities, security during development, delivery security, flow remediation, tools and techniques), 4) tests (functional testing (plans, procedures and records), testing coverage analysis, testing depth analysis, independent testing, 5) vulnerabilities assessment and 6) composition (composition rationale, development evidence, dependent component, base testing, composition vulnerability analysis).

5. System Evaluation

The security measures imposed at the system or infrastructure level are those specified by the ISO 27000 family of standards [16], which pertains to information security management. System-level evaluation and protection can also be achieved by implementing the policies specified in the NIST Cybersecurity Framework (CSF), developed by the National Institute of Standards and Technology. The framework offers a flexible and cost-effective approach to managing cybersecurity risks. It consists of five core functions: identify, protect, detect, respond, and recover. The CSF is widely adopted by organizations to enhance their cybersecurity posture, providing a comprehensive method for managing and mitigating risks. For entities in critical sectors such as energy, transportation, healthcare, and defense, the NCSC Cyber Assessment Framework

(CAF) which is a set of tools and guidelines can be used to ensure cyber resilience.

All this standards cover various aspects of information security, including policies, processes, technical and physical security measures, risk management, auditing, and monitoring. A key concept is the notion of risk [17], which is defined as the product of the impact (I) resulting from an unforeseen event and its effect on the attributes of information security, coupled with the probability that a threat (A) will exploit a vulnerability (V). Therefore, the risk equation is:

$$R = I \times \Pr(A|V).$$

The risk equation described above can also be analyzed from a Bayesian perspective, in the sense that a vulnerability can be exploited by multiple threats, leading to the evaluation of a posteriori probability Pr(V|A):

$$\Pr(V|A) = \frac{\Pr(A|V)\Pr(V)}{\Pr(A)}.$$

In the context of artificial intelligence development, identifying vulnerabilities, threats, and estimating probabilities Pr(A), Pr(V), the a priori probability Pr(A|V), and the posterior probability Pr(V|A) become dynamic processes in determining the appropriate model. It is important to identify and assess both threats and vulnerabilities to gain a comprehensive understanding of risks. This approach aids in developing an effective risk management plan, focusing on mitigating threats and addressing vulnerabilities to enhance system security. The development of a comprehensive list of threats and vulnerabilities is impossible. In this context, the occurrence of a "black swan" event, characterized by a major impact on the system and that can only be explained after its occurrence, is possible. In the context of information security, black swan events refer to unexpected and highly impactful incidents that may have severe consequences for an organization's cybersecurity: zero-day exploits, advanced persistent threats, large-scale ransomware, attacks, supply chain attacks, nation-state cyber operations, emergence of quantum computing threats, large-scale infrastructure failures.

In practice, it is desirable for this risk to be minimized (it cannot be zero because, in such a situation, we would be dealing with a completely closed system, rendering it unusable). Since the value of the impact (I) cannot be minimized, the only action we can take is to reduce the probability value. This can be achieved by imposing additional security controls, incurring additional costs. Therefore, this evaluation must be conducted concurrently with a cost-benefit analysis. The awareness of system vulnerabilities is achieved through the previously specified assessment processes (sections 2-4). A distinct role is played by zero-day vulnerabilities. Within the conducted analyses, penetration tests are mandatory both at the system level and for the developed and utilized applications. The implementation of security controls [18] aims to minimize the risk of undesired events. However, in the event of security incidents, they must be managed [19]. The phases of a security incident are precursors (signs/indicators that such an event is imminent), occurrence, detection, isolation, recovery, and lessons learned. A critical issue is the minimization of the time between its occurrence and its detection. There are situations where this time interval is hundreds of days, as in the case of the APT 38 attack carried out by the Lazarus group [20].

6. Conclusions and future work

This paper has explored four essential aspects of cybersecurity: the theoretical foundations of statistical evaluating cryptographic algorithms, the evaluation and certification of cryptographic modules, the implementation of cryptographic solutions in applications, and the integration of security measures in complex systems. Each of these components is interdependent, contributing to a comprehensive approach to the current challenges in the field of cybersecurity. We emphasize that by interconnecting these four parts, we are working towards the development of a more robust security framework that can be applied in both professional practice and academic research. This framework not only facilitates a better understanding of threats and solutions but also provides clear directions for future research. In the context of future research activities, we will analyze various aspects of cybersecurity, including the evolution of malware threats, with a focus on ransomware. Motivated by pragmatic considerations, we observe a trend of continuous sophistication, which includes the development of 'Ransomware-as-a-Service' (RaaS) models and the identification of new directions in this field.

Another important research direction is trust in emerging technologies, such as 5G communication networks. In implementing these technologies, the evaluation of products and services, following standards like the European Union Cybersecurity Certification (EUCC) for products and European Union Cybersecurity Services (EUCS) for services, is mandatory to ensure security. Additionally, it is necessary to focus on the suitability and security of cryptographic algorithms and modules (both hardware and software) in the face of challenges posed by quantum technologies, such as the Grover algorithm, which dramatically reduces key space. Furthermore, we consider the impact of artificial intelligence (AI) used in cyber operations and the need to adapt to this evolution. To address these challenges, close cooperation between academic institutions, research institutes, and the private sector is mandatory. Collaboration within these entities can facilitate the exchange of knowledge and expertise, as well as expedite the innovation process in developing advanced cybersecurity solutions. An important aspect that could be emphasized is the need for continuous adaptability to address rapidly changing threats in the cybersecurity landscape.

REFERENCES

[1]. *R. Mattioli, A. Malatras, E. N. Hunter, M. G. Biasibetti Penso, D. Bertram, I. Neubert*, "Identifying emerging cyber security threats and challenges for 2030", ENISA, European Union Agency for Cyber Security, March 2023.

[2]. *** Canadian Centre for Cyber Security, An introduction to the cyber threat environment, Communications Security Establishment, Ottawa, ISBN 978-0-660-45950-9, 2022.

[3]. *Y. Li, Q. Liu*, "A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments", Energy Reports, Volume 7, 2021,Pages 8176-8186,ISSN 2352-4847, https://doi.org/10.1016/j.egyr.2021.08.126.

[4]. *S. Chng, H. Yu Lu, A. Kumar, D. Yau*, "Hacker types, motivations and strategies: A comprehensive framework", Computers in Human Behavior Reports, Volume 5, 2022, 100167, ISSN 2451-9588, https://doi.org/10.1016/j.chbr.2022.100167.

[5].*** NIST SP 800-22 Rev. 1, A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications.

[6]. *A. Luengo, E. Román Villaizán*, "Cryptographically Secured Pseudo-Random Number Generators: Analysis and Testing with NIST Statistical Test Suite". Mathematics 2023, 11, 4812. https://doi.org/10.3390/math11234812.

[7]. *A. Bikos, P.E. Nastou, G. Petroudis, Y.C. Stamatiou*, "Random Number Generators: Principles and Applications", Cryptography 2023, 7, 54. https://doi.org/10.3390/cryptography7040054.

[8]. *** EN ISO/IEC 19790:2020 Information technology - Security techniques - Security requirements for cryptographic modules

[9]. *** ISO/IEC 15408-1:2022 Information security, cybersecurity and privacy protection, Evaluation criteria for IT security, Part 1: Introduction and general model

[10]. *** ISO/IEC 15408-2:2022 Information security, cybersecurity and privacy protection, Evaluation criteria for IT security, Part 2: Security functional components.

[11]. *** ISO/IEC 15408-3:2022 Information security, cybersecurity and privacy protection, Evaluation criteria for IT security, Part 3: Security assurance components.

[12]. *** P. Nowak, O. Hryniewicz, "On Some Laws of Large Numbers for Uncertain Random Variables", Symmetry 2021, 13, 2258. https://doi.org/10.3390/sym13122258

[13]. *Z. Qu, Z. Zong, F. Hu*, "Law of Large Numbers, Central Limit Theorem, and Law of the Iterated Logarithm for Bernoulli Uncertain Sequence". Symmetry 2022, 14, 1642. https://doi.org/10.3390/sym14081642

[14]. *** FIPS 140-3 Security Requirements for Cryptographic Modules, https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-3.pdf (accessed 20 decembre 2023)

[15]. *H. Krawczyk*, "The Order of Encryption and Authentication for Protecting Communications (or: How Secure Is SSL?)", In: Kilian, J. (eds) Advances in Cryptology — CRYPTO 2001. CRYPTO 2001. Lecture Notes in Computer Science, vol 2139. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-44647-8_19

[16]. *** ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection, Information security management systems.

[17]. *** NIST Special Publication 800-30 Revision 1, Guide for Conducting Risk Assessments, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf (accessed 12 December 2023).

[18]. *** NIST SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations, https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final (accessed 12 December 2023).

[19]. *** ST Special Publication 800-61 Revision 2, Computer Security Incident Handling Guide, https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf (accessed 12 December 2023).

[20]. *** PT38: Details on New North Korean Regime-Backed Threat Group. Available online: https://www.mandiant.com/resources/blog/apt38-details-on-new-north-korean-regime-backed-threat-group (accessed 12 December 2023).