OPINION

by Dr. Eng. Todor Stoyanov Djamiykov, Professor at the Technical University – Sofia
on a dissertation for the award of the educational and scientific degree "Doctor"
in: Field of Higher Education 5. Technical Sciences;
Professional Direction 5.3 Communication and Computer Technology.
Doctoral Program "Automation in Areas of the Non-Material Sphere (Medicine, Education, Science, Administration, etc.)"

Author: Ivaylo Detelinov Uzunov
Title: Simulation Model and Final Solutions for Security Systems
Supervisor: Prof. Dr. Eng. Slavi Yasenov Lyubomirov

1. General Overview of the Procedure and the Doctoral Candidate

By Order No. RD-22-534/25.02.2025 of the Rector of Plovdiv University "Paisii Hilendarski" (PU), I was appointed as a member of the scientific jury to oversee the defense procedure of the dissertation titled "Simulation Model and Final Solutions for Security Systems" for the award of the educational and scientific degree "Doctor" in the field of Higher Education 5. Technical Sciences, Professional Direction 5.3. Communication and Computer Technology, Doctoral Program "Automation in Areas of the Non-Material Sphere (Medicine, Education, Science, Administrative Activities, etc.)". The author of the dissertation is M.Sc. Eng. Ivaylo Detelinov Uzunov.

The set of materials submitted by M.Sc. Eng. Ivaylo Detelinov Uzunov on paper complies with Article 36 (1) of the Regulations for the Development of Academic Staff at PU and includes the following documents: an application to the Rector of PU to initiate the dissertation defense procedure; a curriculum vitae in European format; a protocol of the preliminary discussion at the department; an abstract; a declaration of originality and authenticity of the submitted documents; a certificate of compliance with the minimum national requirements; a list of publications; the dissertation; copies of publications related to the dissertation.

Ivaylo Detelinov Uzunov completed his secondary education from 2000 to 2005 at the Professional High School of Construction and Architecture in Smolyan. Subsequently, in 2016, he graduated from the Technical College in Smolyan, earning a Professional Bachelor's degree in Computer and Communication Systems. In 2019, he obtained a Master's degree in Engineering with a specialization in "Telematics" from Plovdiv University "Paisii Hilendarski". From 2021 to 2024, he was a regular doctoral student at the Department of EIKIT at Plovdiv University "Paisii Hilendarski".

M.Sc. Eng. Ivaylo Uzunov began his professional career in 2016 as a technician in a mobile phone repair service. From 2020 to 2021, he worked as an assistant at Plovdiv University "Paisii Hilendarski", Faculty of Physics and Technology. Since 2022, he has been employed as a computer systems technician at IT System.

2. Relevance of the Topic

The dissertation is dedicated to simulation models and final solutions in security systems. It covers a broad spectrum of topics: analysis of cryptographic algorithms such as AES and RSA, various types of cyber threats like phishing, SQL injections, DoS attacks, and mal-

ware, as well as methods for their prevention. A significant part of the work describes simulations conducted in MATLAB to illustrate attack principles and the effectiveness of defense mechanisms. An extensive review of existing literature in the field of information security and simulation models for training and analysis of network systems is also provided. The appendices include detailed MATLAB code for simulating various types of cyberattacks.

The main objective of the dissertation is to explore the possibilities of applying a simulation model and final solutions for security systems. This goal is achieved through additional tasks, which include deriving innovative interpretations of research results, reviewing and analyzing algorithms for identifying threats in computer networks, and proposing a verified algorithm for assessing major threat types, criteria, and impact factors. Another task involves reviewing problems in network security and the protection of valuable information resources, as well as ensuring data integrity.

3. Understanding of the Problem

The first chapter of the dissertation provides an analysis and examines key aspects of information security, such as confidentiality, integrity, and availability of information. Various defense mechanisms are described, including access control, encryption, and information classification. The concept of defense-in-depth is also presented.

The review includes different types of computer threats, such as malware, phishing, MITM attacks, and social engineering. Authentication methods, such as password and hash usage, are also discussed.

Existing sources on the problem are reviewed and interpreted through critical analysis. The literature review covers 143 sources in English, including electronic ones. All sources are current scientific publications from reputable journals and proceedings of international conferences by leading experts in the field.

4. Research Methodology

The methodology adopted in the dissertation aligns with its objectives and includes the following aspects:

- Analysis of the specifics of major threat types;
- Investigation and simulation-based analysis of cryptographic models, including symmetric (AES) and hashing (SHA, MD5) algorithms;
- Network scanning using tools like Nmap and Discover to identify vulnerabilities;
- Analysis of web application vulnerabilities, such as SQL injections and XSS attacks;
- Simulation of various cyberattacks in MATLAB, including DoS, MITM, and Replay/Delay attacks;
- Modeling of defense mechanisms like firewalls through simulations;
- Use of simulation methods such as Monte Carlo and Agent-Based models for risk assessment and attack dynamics analysis.

These aspects demonstrate a comprehensive approach combining theoretical analysis with practical simulations and experimental research.

5. Characteristics and Evaluation of the Dissertation and Its Contributions

The dissertation investigates information security through analyses, simulations, and experiments to identify and mitigate vulnerabilities.

Chapter I presents a literature review of cyberattacks, information and computer security, security procedures, and the dissertation's objectives.

Chapter II analyzes cryptographic models, including symmetric (AES) and asymmetric algorithms, hashing functions (SHA, MD5), and digital signatures, presenting simulation results from MATLAB.

Chapter III examines the security of network information systems, analyzing vulnerabilities through network scanning with Nmap and Discover, phishing attacks (SEToolkit), and web vulnerabilities like SQL injection and XSS.

Chapter IV presents experimental research and simulation models in MATLAB for AES encryption, MITM, Replay and Delay attacks, DoS attacks, probability of successful attacks (Monte Carlo), and Agent-Based models for network security analysis.

The author has presented in the dissertation 3 scientific-applied and 5 applied contributions. I accept that these are reasonably and justifiably proposed based on the work described in the dissertation.

6. Assessment of Publications and Personal Contribution of the Doctoral Candidate

The dissertation by Ivaylo Uzunov is supported by five publications. Four of these are co-authored with the supervisor, and one is independent.

The review of the publications shows that they cover the dissertation's topics and present the achieved results to the scientific community. Their number is sufficient and meets the accepted requirements.

The proposed scientific-applied and applied contributions are reflected in a sufficient volume and content of the candidate's publications. They have been presented at renowned and established scientific forums in the field, indicating that the results have gained recognition in the scientific community. I believe that the candidate's personal contribution is evident and confirmed by the independent publication and co-authorship with the supervisor.

All theoretical and practical statements are well-argued, correct, and methodologically sound. However, minor editorial inaccuracies and omissions can be noted, some of which are:

The introduction states that the dissertation presents a "simulation model and final solutions for security systems of threat types in computer systems." However, in the first two chapters, including the literature review and the simulation analysis chapter, insufficient detailed information is provided about the essence, structure, and characteristics of this proposed model. It is unclear how the literature review directly leads to the definition of the specific simulation model to be used and investigated in subsequent chapters.

The dissertation covers a wide range of topics, from cyber threats and cryptographic models to experimental research with scanning tools and MATLAB simulations. There may be a lack of specific, detailed focus and depth in the study of particular aspects. A more in-depth examination would allow for more exhaustive conclusions and stronger scientific-applied contributions.

7. Abstract

A careful review of the abstract for the dissertation shows full compliance with the requirements for its preparation. It adequately reflects the main points and contributions of the dissertation and fully corresponds to the defined scientific-applied and applied contributions contained in the full text of the dissertation.

In conclusion, the abstract aligns with the dissertation in terms of structure, thematic focus, methodology, and contributions.

8. Recommendations for Future Use of the Dissertation Contributions and Results

The conducted research and proposed scientific-applied contributions are directly applicable in practice. They can be implemented in cybersecurity training programs: The developed MATLAB simulations of cryptographic algorithms (such as AES), models of various attacks (DoS, Replay, Delay, MITM), and Agent-Based models can be integrated into curricula and courses for training cybersecurity specialists.

The presented methods for vulnerability analysis using scanning tools (such as Nmap and Discover), techniques for defense against injection attacks (SQL Injection, PHP Code Injection, OS Command Injection), and models for simulating network attacks and firewalls can be adapted and applied in real corporate and institutional environments.

Conclusion

The dissertation contains scientific-applied and applied results that represent an original contribution to science and meet all the requirements of the Law for the Development of Academic Staff in the Republic of Bulgaria (LDASRB), the Regulations for the Implementation of LDASRB, and the corresponding Regulations of PU "Paisii Hilendarski".

The dissertation demonstrates that the candidate, M.Sc. Eng. Ivaylo Detelinov Uzunov, possesses profound theoretical knowledge and professional skills in the scientific specialty 5. Technical Sciences, Professional Direction 5.3. Communication and Computer Technology, and demonstrates the qualities and abilities to conduct independent scientific research.

For the reasons stated above, I am convinced to give my positive assessment of the research presented in the reviewed dissertation, abstract, achieved results, and contributions, and I propose to the esteemed scientific jury to award the educational and scientific degree "Doctor" to M.Sc. Eng. Ivaylo Detelinov Uzunov in the field of Higher Education: 5. Technical Sciences, Professional Direction 5.3. Communication and Computer Technology, Doctoral Program "Automation in Areas of the Non-Material Sphere (Medicine, Education, Science, Administrative Activities, etc.)".

24.04.2025 Prepared by: .....

(Prof. Dr. Todor Djamiykov)