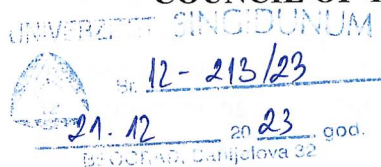


**COUNCIL OF THE DEPARTMENT FOR POSTGRADUATE STUDIES
SINGIDUNUM UNIVERSITY**



Belgrade
Danijelova St. 32

By the decision of the Council of the Department of Postgraduate Studies and International Cooperation of Singidunum University, No. 4-120/2022 of 31 August 2022, we have been designated as members of the Commission for review, evaluation and oral defense of Meiran Galis doctoral dissertation, entitled: **“Contribution to Information Security Continuous Audit in Cloud-Native Environments”**.

After reviewing the submitted dissertation and other supporting materials, the Commission made the following

R E P O R T

1. INTRODUCTION

1.1. Chronology of approval and preparation of dissertation

Meiran Galis enrolled in doctoral study programme Advanced Security Systems at Singidunum University in the school year 2020/2021. He passed all requested exams, with a mean grade of 10. By the Decision of the Council of the Department of Postgraduate Studies of Singidunum University, No. 4-120/2022 of 31 August 2022, the Commission was formed within:

1. Milan Milosavljević, PhD, Full Professor, Singidunum University, Belgrade
2. Mladen Veinović, PhD, Full Professor, Singidunum University, Belgrade
3. Tomislav Unkašević, PhD, Assistant Research Proffesor, VLATACOM Institute, Belgrade

for review, evaluation, and oral defense of Meiran Galis doctoral dissertation, entitled: **“Contribution to Information Security Continuous Audit in Cloud-Native Environments”**.

Based on the positive report of the Commission, the Council of the Department for Postgraduate Studies of Singidunum University approved the work on the preparation of the doctoral dissertation. Prof. Dr. Milan Milosavljević was appointed as a mentor.

1.2. Scientific field of dissertation

This dissertation belongs to the field of Natural sciences and Mathematics, area: Computer Science, for which the Singidunum University is matic.

1.3. Biographical information about the candidate

Meiran Galis was born 03.03.1990 in Israel. He is citizen of Israel. He received his bachelor’s degree in Information Systems from the Academic College of Tel Aviv – Yafo (MTA),

Israel. He received his master's degree in Sinergia University, Bijeljina. His current filled placement is in Information Security for cloud technologies, and audit service organization in various security standards focused on data protection and privacy. He prepared thorough reports on companies' security, confidentiality, availability, processing integrity, and privacy. He has experience with software development lifecycle in agile environments, change management, control access, complex cloud applications, network, host, and virtual system operations. He is interested in cyber risk, IT compliance automation, cryptography, and secure multiparty computation.

2. DISSERTATION DESCRIPTION

2.1. The content of the dissertation

Doctoral dissertation entitled: "Contribution to Information Security Continuous Audit in Cloud-Native Environments". It has 104 pages. The dissertation has six chapters and a list of literature. The chapters are:

1. Introduction, 5 pages,
2. Cloud Computing Technology Overview, 19 pages,
3. Information security principles, 15 pages,
4. Information theory approach to cryptographic parameters generation, 21 pages,
5. EEG based cryptographic keys agreement protocol, 39 pages,
6. Summary, contributions of the research work and further research, 3 pages.

There are a total of 20 figures and 3 tables in the dissertation. The literature contains 71 bibliographic units.

2.2. A brief overview of individual chapters

First Chapter presents the motivation for this research, problem and subject of the research and overview of the dissertation contents.

Second Chapter presents in brief cloud computing technologies, their taxonomy and key features. Also, relationship of cloud based information systems regarding continuous auditing and information security is described. In that context brief introduction into information system auditing will be presented.

Third Chapter of the dissertation describes basic information security principles and cryptographic basis of information security with accent on the randomness of cryptographic parameters. Connection of the cryptographic parameters generation and continuous auditing is described.

Forth Chapter, contains description of Information theory approach to cryptographic parameters generation and its formal model

Fifth Chapter is the central part of the dissertation. In this part Information theory method for common random string establishment based on collected EEG signals aroused by the same mental stimulus between communication participants. Exact method will be presented in this part with theoretical arguments for its correctness. Correctness is based on information theoretic and statistical analysis. Set of parameters which influence length of obtained common random strings

is identified and strategies on choosing parameters values are defined. Results of extensive experimental analysis and conclusion are presented in this chapter.

Sixth Chapter is closing part of the dissertation. In this part summation of the research is presented with achieved goals and results. According to the achieved results contribution of the research is described with potential applications and directions of further research is listed.

At the very end of the dissertation is a list of references.

3. DISSERTATION GRADE

3.1. Modernity and originality

Modern information technologies and globalization have dramatically changed today's world of computer networks, which are characterized by a high degree of integration of various electronic services. As the number of Internet services and new users of services increases every day, the amount and value of information exchanged increases. Information exchanged over networks and storage on networked memory locations may be compromised if not adequately protected.

In the digitalized world and Cyberspace, as symbiotic community of men and machines, Cloud computing technologies and digital services based on them have important role in everyday life and business processes.

Increasingly enterprises are incorporating cloud-based applications into their regular business operations. In order to protect their confidential data, if required by legal commitments or if by regulations, they need to verify that their IT vendors follow relevant security standards and privacy regulations.

From an information security standpoint, a whole range of security challenges arise, starting with security goals and security architecture through their operationalization and implementation. This is particularly reflective of the information security audit as part of the audit of information systems. In terms of information security cryptographic algorithms and cryptographic protocols are significantly standardized and support the approach of continuous external audit and improvement of the security of the subject information system. On the other hand, all of these solutions involve the use of cryptographic parameters created appropriately and under certain conditions. This audit segment requires specialist knowledge and the ability to assess the adequacy of the procedures applied. Contrary to cryptographic algorithms and protocols in this segment, there is no generally accepted standardization.

The research of this doctoral dissertation resulted in the development of an advanced solution for the establishment of the cryptographic parameters using non-uniform random sources. This contribution includes substantial changes to the usual system architecture allowing elimination trusted third parties from the process and establishment of end-to-end cryptographic protection in communication. This research developed a method that would be reliable in theoretical terms and proofs and also independent of trusted third parties. Such a method would significantly improve the possibilities of continuous revision in this segment and information security in the systematic sense.

In this context, the candidate confirmed his originality in a correct and convincing way by publishing papers in international scientific journals (1 paper in an impact factor journal), in domestic scientific journals (1 paper) and in proceedings from international scientific conferences (2 papers).

3.2. Review of reference and used literature

In the preparation of the dissertation, extensive literature in the field of protocols for generation cryptographic parameters and continuous auditing of cloud computing technologies was used, up to the latest papers in top international scientific journals, including their own references. Based on these references, the original scientific results obtained by the candidate in the dissertation are placed in a correct context.

3.3. Description and adequacy of applied scientific methods

During the scientific and research work, the candidate used various methods in order to meet the basic methodological requirements – objectivity, reliability, generality and systematics.

In accordance with the chosen problem, defined research goals and set scientific hypotheses in order to define scientific and professional conclusions and find possible solutions, theoretical analysis was used using research results from international scientific literature, i.e. the knowledge of scientists and other authors who investigated the problem that this paper deals with. The dissertation presents scientific and theoretical knowledge, relevant literature and original proposals using a number of methods, namely: historical methods, methods of complex observation and analysis of content, methods of analysis and synthesis, methods of proof, as well as experimental methods.

Using the historical method, the results of research by other authors who dealt with issues related to topics of interest were obtained. The data obtained mainly come from eminent scientific papers and research in this area.

The method of complex observation and content analysis was applied when processing the results taken from the research of other researchers. The results were used in order to define the shortcomings of existing algorithms of automatic classification of modulation and to determine the direction for potential improvements.

The main challenge solved by this doctoral dissertation was achieved through the development of protocol for establishment cryptographic parameters based on non uniform sources of randomness in the presence of eavesdropper whose result are cryptographic keys with uniform distribution and theoretically proved security.

In order to check the effectiveness and efficiency of the proposed solutions, extensive experimental checking is done that confirmed the initial hypotheses of the dissertation.

3.4. Applicability of results achieved

The results and solutions that the candidate has come up with in his dissertation have significant practical significance and application in real conditions and applications. The importance of the presented achievement is sufficiently illustrated by the importance of information security in the everyday life of a digitized society, on which the proposed solution has a direct impact. By applying this solution, cryptographic systems with absolutely secure and random cryptographic keys can be implemented in information systems without the influence of a trusted third party.

Its application can be crucial in areas such as national security, Information protection and cybersecurity as well as in research and development of new technologies in the field of protocols for establishment of the cryptographic parameters.

3.5. Assessment of the achieved abilities of candidates for independent scientific work

In his previous work, the candidate has demonstrated qualities crucial for successful research work: the ability to spot problems and set a correct research goal, understanding and expanding theoretical concepts, originality, the ability to translate theoretical methods into algorithms, as well as to critically analyze the obtained results.

4. SCIENTIFIC CONTRIBUTION

4.1. An overview of the scientific contributions

Based on this dissertation all the set goals that the dissertation was supposed to evaluate have been achieved. The main contributions of the dissertation are as follows:

The dissertation is based on the synthesis of the publicly known facts and achievements of well-known scientists. The main contribution of this dissertation in the field of symmetric key establishment protocol is the following:

- Synthesis of the Information theory methods and correlated individual biometrical signals into the novel secure protocol for symmetric secret key establishment.
- Defined protocol allows key establishment for the symmetric cryptographic systems directly between participants in communication.
- In the cloud computing environment improve security and reduce the system complexity by elimination significant part of the key management system performed by the trusted third party.
- Providing highly secure end-to-end communication in cloud computing security improve general security in the cyberspace.
- Allow outsourced auditing of the security in the information systems.
- Reduce complexity and cost of the information system security auditing.

4.2. Critical analysis of research results

In the first phase, the candidate, considering the available literature in the field of the dissertation topic, performed a critical analysis of the available information and correctly defined the goal of the research. During his research work, he used the possibility of critical review and suitable ways of improving existing solutions by adding his contribution through new ideas. The proposed model of solution to the problem was practically implemented and experimentally obtained the results of modeling with appropriate reference values (results of computer simulations). The advantages and disadvantages of the proposed approach are observed and presented and the guidelines of possible further research are pointed out.

4.3. Verification of scientific contributions

The scientific contributions of the dissertation are verified by the following papers of the candidate:

Published papers in journals of category M22:

1. **Galis, M.**; Milosavljević, M.; Jevremović, A.; Banjac, Z.; Makarov, A.; Radomirović, J. Secret-Key Agreement by Asynchronous EEG over Authenticated Public Channels. *Entropy* 2021, 23, 1327. <https://doi.org/10.3390/e23101327>

Published papers in journals of category M51:

1. **Galis, Meiran**, Unkašević, Tomislav, Banjac, Zoran, Milosavljević, Milan, Protocols for symmetric secret key establishment: Modern approach 2022 *Vojnotehnički glasnik*, Vol. 70, No. 3 pp. 604-635

Published papers in proceedings of international conferences of category M33:

1. **Galis, M.**, T. Unkašević, Z. Banjac and M. Milosavljević, *Automated Compliance System for Ser Vice Organizations*, Univerzitet Singidunum, Beograd, 2021, doi:10.15308/Sinteza-2021-21-27
2. **Galis, M.**, T. Unkašević, M. Milosavljević, Z. Banjac and P. Milosav, "Modern techniques for decentralized key establishment in symmetric cryptographic systems," 2021 29th Telecommunications Forum (TELFOR), 2021, pp. 1-4, doi: 10.1109/TELFOR52709.2021.9653401.

5. OPINION OF THE COMMITTEE MEMBERS

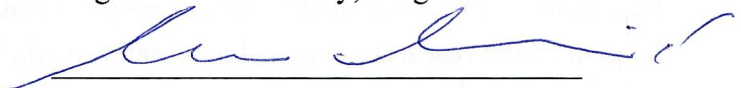
We assess that the candidate **Meiran Galis**, provided a PhD research thesis entitled: "Contribution to Information Security Continuous Audit in Cloud-Native Environments" that is scientifically relevant. Also, we find that the main concepts are well defined, the application of the methods are presented, that the dissertation consists of all necessary elements and that writing is concise. We consider that the candidate has done a PhD dissertation on the proposed topic in accordance with the given research goals.

In this context, we conclude that the PhD dissertation is valuable to be defended. Therefore, we propose to the Department for Postgraduate Studies of Singidunum University of Belgrade to approve the candidate **Meiran Galis** to defend his PhD dissertation under the title: "**Contribution to Information Security Continuous Audit in Cloud-Native Environments**".

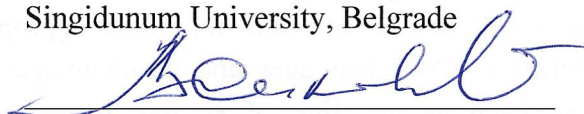
Belgrade, 14.12.2023

Members of the Commission:

Dr. Milan Milosavljevic, full professor,
Singidunum University, Belgrade



Mladen Veinović, PhD, full professor,
Singidunum University, Belgrade



Dr. Tomislav Unkašević, Research Associate
Professor,
Vlatacom Institute, Belgrade

