REVIEW

on a dissertation for obtaining the educational and scientific degree "Doctor" in the field of higher education 4. Natural sciences, mathematics and informatics, professional field 4.6 Informatics and computer sciences

Author of the dissertation: Tihomir Dimitrov Tenev

Dissertation topic: Development of a hierarchical taxonomy of models for improving security in information systems based on microservice architecture

Reviewer: Prof., Dr. Vladimir Todorov Dimitrov, FMI, University of Sofia St. Kliment Ohridski

1. Relevance and significance of the problem developed in the dissertation

The topic of the dissertation is in the field of computer security and in particular computer security in the architecture of microservices. According to the literature source [3] of the dissertation:

"In short, the microservice architectural style is an approach to developing a single application as a suite of small services, each running in its own process and communicating with lightweight mechanisms, often an HTTP resource API. These services are built around business capabilities and independently deployable by fully automated deployment machinery. There is a bare minimum of centralized management of these services, which may be written in different programming languages and use different data storage technologies."

Architectural style is a means for architecture implementation. For example, a client-server architecture can be implemented through the architectural style of microservices.

The title of the dissertation points to the information system security, but the examinations show that the investigations are not limited only in this direction.

The research in the dissertation is for the development of a hierarchical taxonomy of security models. The resulting taxonomy does not have to be hierarchical.

I define the topic of the dissertation as follows: “Taxonomizing of security patterns in the architectural style of microservices”. From this starting point, I consider the relevance and significance of the dissertation.

In the first place, the problems of computer security in modern society have been significantly replaced only by the COVID-19 pandemic. The failures in the security of software systems are increasing every year, which is related to their comprehensive and in-depth penetration into our daily lives, as well as to the growing complexity of the applications.

On the second place is the emergence of a new architectural style of microservices. This style originated from the Linux environment as a means of protecting namespaces in the operating system.

Below I will use “microservice architecture” for short instead of “microservice architectural style”.

Although it is a completely new style, it quickly found the support of a number of leading software vendors. The reason for this is rooted in the demonstrated advantages over existing architectures and architectural styles.

The concept of the considered architectural is characterized by the pair container-docker. In fact, the microservices are packaged in containers and delivered to the dockers for execution. The latter can be deployed on both physical and virtual machines. The containers, on the other hand, are as compact as possible - they contain only a microservice code and a description of the runtime environment. This makes the container hundreds and even thousands of times smaller than a virtual machine and easily transfers to the network from one place to another.

The microservice architecture is a development of service-oriented architecture (also architectural style). The scope and applicability of the microservices architecture, at least for now, is not clear, but it is clearly promising and is likely to revolutionize service delivery.

Unfortunately, any new technology suffers from a lack of security - vendors are rushing to deliver functionality while ignoring security. The case with the architectural of microservices is not different, which outlines the relevance of the research in the dissertation.

2. General characteristics and structure of the dissertation

According to the dissertation, “The aim of the dissertation is to develop a hierarchical taxonomy of models for improving security in software systems based on microservice architecture.” The comments above on the title are also valid for this formulation of the purpose; I will only add that the object of study is more precisely reflected here, namely “software systems” and not “information systems” as in the title.

The set tasks for achieving the goal, according to the dissertation, are:

“1. To categorize and granulate a new generation software architecture, also called Microservice architecture, in order to present it in different forms.

2. To make a threat analysis for each of the presented categories of microservice architecture.

3. To find appropriate security models that fall within the scope of the different categories, relying on the analysis of threats.

4. To transform the justifications and solutions provided by the different security models to the context of the wet service architecture.

5. To make a hierarchical model of all categories of microservice architecture, which will serve as a skeleton in the construction of a detailed hierarchical taxonomy.

6. To find and use an appropriate object-oriented modeling language in order to make the selected security models readable, respecting the hierarchy of the individual categories.

7. Transform the modeling language so that it can be represented graphically.

8. To find modern products with the help of which a sustainable environment for microservice application can be created.

9. To study which of the presented security models can be applied by means of the selected modern products for management of microservice applications, as well as to give an example solution.”

I will analyze each of the tasks. The latter should look like this:

1. Study of the architecture of microservices and its realizations.
2. Analysis of general and specific threats to the architecture of microservices.
3. Collection of security patterns applicable to the microservices architecture. Choice of threat system. Systematization of security patterns according to the threat system.
4. Formulation of security patterns in terms of microservice architecture.
5. Building a taxonomy of security patterns for microservice architecture.
6. Selection and application of a language for describing the taxonomy. The latter must have graphic visualization capabilities.
7. Graphic visualization of the taxonomy.
8. Selection of environment for development of an exemplary solution with the architecture of microservices. Development of the sample application.
9. Application of security patterns to the sample solution.

Simply put:

- to study the architecture of microservices;
- to collect the security patterns applicable to it and to reformulate it in its terms;
- to select a system for classification of the security patterns and to classify them latter according to the system;
- to choose a language for describing the taxonomy allowing graphic visualization;
- to graphically visualize the taxonomy;
- to select an environment and an example application for the microservice architecture;
- and attach the security templates to the sample application.

The introduction, in essence, contains a brief description of the chapters of the dissertation.

Chapter 1 is an introduction with references to literature on microservice architecture. It is informal and with different levels of abstraction. Here is the author's view of architecture.

This chapter lists the STRIDE threat classification system. This is Microsoft's system for classifying threats into application categories developed by the company.

This chapter also provides a brief the CIM description. This is a tool for describing and managing objects in information technology environments.

The visualization of the CIM descriptions is pointed out to be performed with UI Wireframing. Graphical representation of CIM models is provided by standard in the form of UML diagrams, for which the corresponding stereotype has been developed.

At the end of the chapter are formulated the purpose and objectives of the dissertation, which were commented above.

The following chapters, from 2 to 6, deal with the security patterns in the following design (architectural) patterns: account and identity, communication, persistent data, environment, third party suppliers.

Each of these chapters begins with an informal description of the design template and discusses the specifics of STRIDE threats. This is followed by a reference to a publication in which the security patterns are collected according to the given design-technological pattern. This is a reference to the doctoral student's publication (jointly with a supervisor or independently). The following is a comment for each security pattern in the STRIDE direction.

Finally, the chapter ends with a conclusion.

The comments on the security patterns are based on the architecture proposed by the author.

Chapter 7 gives a brief description of CIM. The idea is to describe security patterns with CIM as objects.

The taxonomy is presented as a hierarchy, which is organized according to the proposed architecture.

The visualization of the taxonomy is made in the form of tables. The first dimension is security patterns, and the second is STRIDE. One table is displayed for each design-technological pattern.

The security pattern is described with the attributes Pattern (there is a security pattern), Context (application context), Solution (solution description), STRIDEAccronim (threat classification or STRIDE threats) and Reference (source of the threat pattern).

In Chapter 8, the taxonomy is applied to the detailed architecture of the prototype solution. Here, the security patterns of the design patterns are related to specific software components of the software solution. The specific developments on the security patterns are presented.

Chapter 9 is a half-page conclusion.

Chapter 10 is about the contributions of dissertation work. There are 6 of them, which I comment on in the relevant section of the review.

Chapter 11 is a declaration of originality.

The full text of the taxonomy in CIM is attached in Chapter 12.

Chapter 13 is for the literature used. These are 111 sources, mostly from the Internet.

3. Degree of penetration into the problem and assessment of the state of its solution now

The architecture of microservices is very new and the views of different authors vary considerably.

Microsoft's STRIDE classification is not the only approach to threats - the level is too high. In general, threats are detailed as vulnerabilities, weaknesses and patterns of attacks. At the same time, vulnerabilities are “typified” by weaknesses, and for weaknesses and attacks there are highly developed and established taxonomies by purpose.

The results obtained in the dissertation are valid for the considered architecture (not for the architectural style of the microservices). They cannot be summarized for the microservice architecture. The solutions proposed in the dissertation are private.

4. Regarding the chosen research methodology

There is no research methodology formulated in the dissertation. The approach to research is purely engineering.

An architecture with certain design patterns is presented and security patterns are attached to it. Security patterns are classified according to the design patterns and the latter are characterized according to the threats from STRIDE. The security patterns are reduced to the design - technological patterns. Finally, the architecture is detailed to a project with specific software components, and in the detail, the security patterns are specified to code.

5. Brief analytical description of the nature and reliability of the material on which the contributions of the dissertation are built

The dissertation is 151 pages long. It consists of an introduction, 8 chapters, a conclusion, contributions, a declaration of originality, appendices, references and a list of publications on the dissertation. The literature used includes 111 titles in English. Of the publications, 49 are from conference and publication materials, the remaining 52 are from Internet sources.

The introduction is 2 pages, Chapter 1 - 11, Chapter 2 - 12, Chapter 3 - 20, Chapter 4 - 7, Chapter 5 - 10, Chapter 6 - 8, Chapter 7 - 15, Chapter 8 - 15, Conclusion - 1, Contributions - 1, Declaration of originality - 1, Appendices - 28, References - 8, List of dissertation publications - 1.

The main elements on which the dissertation is built are the architectural patterns and the security patterns.

The architectural patterns are technologically fixed in the dissertation - these are design-technological patterns. Architecture as a technological solution is fixed by the doctoral student. These patterns are well known as well as their technological implementations. In the dissertation, they are combined in an engineering solution.

The security patterns in the dissertation are taken from sources in which the author or co-author is the doctoral student. The sources for each individual security pattern are indicated.

6. Main scientific and scientific-applied contributions in the dissertation

The contributions of the dissertation are listed as follows (numbering is by me):

1. Research and analysis of architectures based on microservices has been performed in order to increase security.

2. A conceptual model is proposed, applying microservice architecture, with the help of which they are Graphical.

3. An analysis of the threats on the defined vulnerable areas has been performed, for each of which appropriate security models and the justification of the decisions have been proposed.

4. A hierarchical model is developed and a hierarchical taxonomy of security models is presented with the help of object-oriented modeling.

5. A graphical interface has been developed that illustrates the connections between vulnerable areas in the microservice architecture and the selected security models.

6. The architecture of a platform implementing the proposed models is presented, using modern technologies for microservice management.

By contribution 1, the author became acquainted with microservice architectures and a number of security patterns.

By contribution 2, the author has defined an architecture based on six design-technological patterns. The meaning of Graphical is unclear.

According to contribution 3, a classification of the security patterns according to STRIDE and according to the design-technological patterns has been made. The security patterns are commented in the context of the technologies of the architectural (design-technological) patterns.

Contribution 4 created a CIM taxonomy of security patterns in the form of configuration management objects. The taxonomy is hierarchical in the sense of the proposed architecture.

According to contribution 5, the developed taxonomy is visualized in the form of tables according to the design-technological patterns.

Contribution 6 presents a component-detailed solution of the architecture from the dissertation with detail to code level or configuration of the security patterns.

7. Evaluation of the author's participation in receiving the contributions

The originality of the submitted work can be judged by the declaration of originality. The dissertation publications are co-authored with either the supervisor or independent. There are no contribution statements in these publications. Taking into account the circumstances and from what is stated in the dissertation, it can be concluded that the contributions to the dissertation are the work of the doctoral student. The role of supervisors was rather methodological.

8. Evaluation of the dissertation publications

5 publications are presented on the dissertation:

1. Tihomir Tenev, Dimitar Birov, Security Patterns for Microservice Account and Identity, In proceedings of the 15th International Conference on Informatics and Information Technologies, 2018, pages: 124-128, ISBN: 978-608-4699-08-8,
2. Tihomir Tenev, Dimitar Birov, Security Patterns for Microservice Communication, Reports of the Forty-seventh Spring Conference of the Union of Mathematicians in Bulgaria, 2018, ISSN (online): 1313-3330
3. Tihomir Tenev, SECURITY PATTERNS FOR MICROSERVICE DATA MANAGEMENT, In proceedings of Doctoral Conference: Young Scientists, 2018, pages: 575-581, ISBN: 978-954-07-4611-1
4. Tihomir Tenev, Dimitar Birov, SECURITY PATTERNS FOR MICROSERVICES LOCATED ON DIFFERENT VENDORS, VII International Conference on Engineering, Technologies and Systems TECHSYS 2018, Technical University - Sofia, Plovdiv, 2018, pages: 130-133, ISSN (online): 2535 -0048
5. Tihomir Tenev, Simeon Tsvetanov, Enhancing security in Microservice environments, 9th Balkan Conference in Informatics, ISec2019 Workshop, 2019

Publication 1 is at an international conference in Northern Macedonia and is cited as [27] in the bibliography.

Publication 2 is cited as [42] in the bibliography.

Publication 3 is cited as [54] in the bibliography.

Publication 4 is cited as [65] in the bibliography.

Publication 5 was published in the journal Computer and Communications Engineering, Vol. 13, no. 4, 2019 and is cited as [59] in the bibliography.

These publications are the basis of Chapters 2-6. The main results of these chapters have been published.

9. Use of the results obtained in the dissertation and recommendations for their future implementation

The results obtained, as they are, can be used in safety studies of micro-service architecture. No less factology has been accumulated.

10. Regarding the abstract to the dissertation

The abstract to the dissertation is 40 pages. The main part of the content of the dissertation is presented in it.

11. Critical remarks

The dissertation is not well designed.

The numbering of the individual parts of the dissertation is eclectic and confusing. For example, Introduction is a separate part, but CONCLUSION is number 9.

The referenced literature is reduced to an unnecessarily low level. For example [26] is Gmail.

Most of the terminology has not been translated from English. Where an English translation has been made, this has been done very badly. For example, "A Pattern for WS-Trust" has simply not been translated, and the term "pattern" has been translated in many places as a "model".

The text of the dissertation lacks an overview and analysis of the studied areas: the architecture of microservices and the threats to software systems.

12. Other issues

I do not know the doctoral student personally.

The formation of the dissertation, due to the death of the research supervisor Assoc. Prof. Dimitar Birov, was undertaken in the last stage by Assoc. Prof. Simeon Tsvetanov.

On the other hand, the atmosphere in the department did not help to refine the dissertation.

13. Conclusion

The dissertation presented by the author satisfies the requirements of ZRASRB, PZRASRB, PURPNSZADSU and PURPNSZADSUFMI. I do not know and I have not found plagiarism in the presented material. I recommend to the esteemed jury to allow Tihomir Dimitrov Tenev to defend the educational and scientific degree “Doctor” in the field of higher education “4.5 Natural Sciences, Mathematics and Informatics”, professional field “4.6 Informatics and Computer Science” and I recommend a positive assessment.

Recoverable Signature

X Владимир Димитров

Date: June 26, 2020 Reviewer: Signed by: Vladimir Todorov Dimitrov

....

Sofia (Prof., Dr. Vladimir Dimitrov)