SILESIAN UNIVERSITY OF TECHNOLOGY

FACULTY OF AUTOMATIC CONTROL, ELECTRONICS AND COMPUTER SCIENCE

Master thesis

Security anomaly detection based on Windows Event Trace

author: Maksym Brzęczek

supervisor: Błażej Adamczyk, PhD

consultant: Name Surname, PhD

Gliwice, September 2020

załącznik nr 2 do zarz. nr 97/08/09

Oświadczenie

Wyrażam zgodę / Nie wyrażam zgody* na udostępnienie mojej pracy dyplomowej / rozprawy doktorskiej*.

Gliwice, dnia 2 września 2020

.....
(podpis)

.....
(poświadczenie wiarygodności
podpisu przez Dziekanat)

* podkreślić właściwe

Oświadczenie promotora

Oświadczam, że praca „Security anomaly detection based on Windows Event Trace" spełnia wymagania formalne pracy dyplomowej magisterskiej.

Gliwice, dnia 2 września 2020

.....

(podpis promotora)

Contents

Chapter 1

Introduction

- introduction into the problem domain
- settling of the problem in the domain
- objective of the thesis
- scope of the thesis
- short description of chapters
- clear description of contribution of the thesis's author

Chapter 2

[Problem analysis]

- problem analysis, problem statement
- state of the art, literature research (all sources in the thesis have to be referenced [1, 2, 3])
- description of known solutions, algorithms
- location of the thesis in scientific domain
- The title of this chapter is similar to the title of the thesis.

Chapter 3

[Subject of the thesis]

- solution to the problem proposed by the author of the thesis
- theoretical analysis of proposed solutions
- rationale of applied methods, algorithms, and tools

Chapter 4

Experiments

This chapter presents the experiments. It is a crucial part of the thesis and has to dominate in the thesis. The experiments and their analysis should be done in the way commonly accepted in the scientific community (eg. benchmark datasets, cross validation of elaborated results, reproducibility and replicability of tests etc).

4.1 Methodology

- description of methodology of experiments
- description of experimental framework (description of user interface of research applications – move to an appendix)

4.2 Data sets

- description of data sets

4.3 Results

- presentation of results, analysis and wide discussion of elaborated results, conclusions

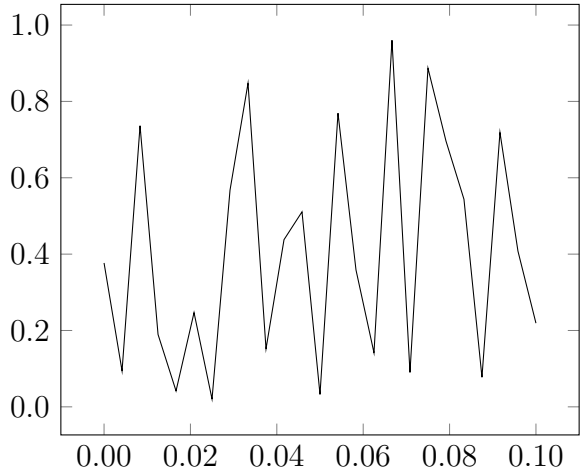

Figure 4.1: A caption of a figure is **below** it.

Table 4.1: A caption of a table is **above** it.

	method						
			alg. 3			alg. 4, $\gamma = 2$	
ζ	alg. 1	alg. 2	$\alpha = 1.5$	$\alpha = 2$	$\alpha = 3$	$\beta = 0.1$	$\beta = -0.1$
0	8.3250	1.45305	7.5791	14.8517	20.0028	1.16396	1.1365
5	0.6111	2.27126	6.9952	13.8560	18.6064	1.18659	1.1630
10	11.6126	2.69218	6.2520	12.5202	16.8278	1.23180	1.2045
15	0.5665	2.95046	5.7753	11.4588	15.4837	1.25131	1.2614
20	15.8728	3.07225	5.3071	10.3935	13.8738	1.25307	1.2217
25	0.9791	3.19034	5.4575	9.9533	13.0721	1.27104	1.2640
30	2.0228	3.27474	5.7461	9.7164	12.2637	1.33404	1.3209
35	13.4210	3.36086	6.6735	10.0442	12.0270	1.35385	1.3059
40	13.2226	3.36420	7.7248	10.4495	12.0379	1.34919	1.2768
45	12.8445	3.47436	8.5539	10.8552	12.2773	1.42303	1.4362
50	12.9245	3.58228	9.2702	11.2183	12.3990	1.40922	1.3724

Chapter 5

Summary

- synthetic description of performed work
- conclusions
- future development, potential future research
- Has the objective been reached?

Bibliography

[1] Name Surname and Nama Surname. Title of an article in a journal. *Journal Title*, 157(8):1092–1113, 2016.

[2] Name Surname and Name Surname. *Title of a book*. Publisher, Hong Kong, 2017.

[3] Name Surname, Name Surname, and N. Surname. Title of a conference article. In *Conference title*, pages 5346–5349, 2006.

Appendices

Technical documentation

List of abbreviations and symbols

DNA	deoxyribonucleic acid
MVC	model–view–controller
N	cardinality of data set
μ	membership function of a fuzzy set
$\mathbb{E}$	set of edges of a graph
$\mathcal{L}$	Laplace transformation

Contents of attached CD

The thesis is accompanied by a CD containing:

- thesis (`pdf` file),
- source code of applications,
- data sets used in experiments.

List of Figures

List of Tables