USB- PORT RISK ANALYSIS AND MONITORING

Kodolányi János University Indrustial engineering- computer science major

Name: Zoltán Lehrer

ORCID: 0009-0002-4978-7492

Neptun code: FY3Z2H

Mentor: Dr. László Pitlik

Keywords: System modelling / Human behaviour and communication/ Data visualization

School year: 2023/2024 II. semester

Contents

1 Extract 3

2. Abstract 4

3. Introduction 6

  3.1. Goals 6

  3.2. Task 6

  3.3 Target groups 7

  3.4 Usefulness 7

4. Literary/ own history 8

  4.1. VID/ PID identifier 9

  4.2. OAM 9

  4.3. The OAM characterization with ChatGPT 9

5. Analysis 11

  5.1. Objects 12

  5.2. Attributes 12

  5.3. Ranking 12

6. Discussion 17

7. Conclusions 17

8. Vision 17

9. Attachments 17

  9.1. List of abbreviation: 17

  9.2. References 18

  9.3. List of figures 18

1 Extract

The topic of my thesis was inspired by the presentation of a USB device that is capable of running a short line of code hidden on it on a computer, and the executed line of code can even endanger our personal data. This is a simple data/charging cable that can cause huge damage to the unsuspecting user. Its users can abuse our personal data, break into computer networks, steal our identity, commit financial fraud, spread malware and viruses, and carry out various types of Internet abuse, harassment or blackmail.

The risk assessment aims to produce a time-series system state risk and treat the symptoms. Risk analysis is an important step in the development and implementation of any project plan. The application of the object-attribute matrix (OAM) enables a structured and comprehensive/optimized analysis of risks, which helps to identify, evaluate (cf. diagnosis) and treat (cf. therapy) potential hazards and uncertainties. OAM is a structure that allows objects (such as project phases, business processes, tools, processes, etc.) and their associated attributes (such as measurable factors, hazards, impacts, etc.) to be linked in a form that supports automated processing. As a result, it is easier to identify and assess potential risks and design appropriate risk management strategies.

The USB port risk analysis enables detailed monitoring and analysis of the activity of USB ports. The data required for the analysis is collected manually from the performance measurement program of the operating system, thereby guaranteeing reliable and accurate results. The process can be automated in the future, which will be explained in more detail in the future description.

Measured values include maximum paging file utilization, disk drive write rate, and CPU and memory utilization. These data are recorded in an object attribute matrix, where the rows show the measured values, these are the objects, while the columns show the elapsed time, these are the attributes. All measurements are made in a two-second time interval, thus ensuring the foundation of a detailed and up-to-date analysis. Based on the raw OAM, we rank and evaluate the various risk factors related to each object as attributes. This enables an objective/optimized exploration of risks. During the analysis, we use the COCO Y0 method, which can be found the https://miau.my-x.hu/myx-free/coco/beker_y0.php on page.

At the end of the analysis, we perform a validity/authenticity test, which is prepared with the inverse version of the original OAM. The analysis is successful if the inverse of the original results is obtained.

It is important that our data is safe on our own devices, such as computer, laptop, smartphone, tablet. The security of our data is closely related to the protection of our privacy and personal information.

In the online space, we often encounter data theft attempts, hacker attacks or other data security threats. If our data is not secure, it is easily exposed to unauthorized access, which can compromise our identity, financial situation, or even personal relationships.

Losing or damaging our data can cause many inconveniences, be it work, personal documents, photos or other important files.

The protection of our data is not only important from the point of view of our privacy, but also from a financial point of view. Unauthorized access to our financial data (banking information, credit card data, etc.) can pose a significant risk to our financial stability.

If we also store data for business or professional purposes on our computer, their security can be vital for our business or workplace. In case of data loss or data theft, it can significantly affect not only individual work, but also the operation of the company.

Keeping our data safe on our own computer is extremely important not only from a personal, but also from a financial, business and legal point of view.

2. Abstract

The topic of my thesis was inspired by the presentation of a USB device that is capable of running a short line of code stored hidden on a computer, and the executed line of code can even endanger our personal data. This is a simple data/charging cable that can cause huge damage to the unsuspecting user. Its users can abuse our personal data, break into computer networks, steal our identity, commit financial fraud, spread malware and viruses, and carry out various types of Internet abuse, harassment or blackmail.

Risk analysis is an important step in the development and implementation of any project plan. The application of the object-attribute matrix (OAM) enables a structured and comprehensive/optimized analysis of risks, which helps to identify, evaluate (cf. diagnosis) and treat (cf. therapy) potential hazards and uncertainties. OAM is a structure that enables objects (such as project phases, business processes, tools, processes, etc.) and their associated attributes (such as measurable factors, hazards, impacts, etc.) to be linked in a form that supports automated processing. As a result, it is easier to identify and assess potential risks and design appropriate risk management strategies.

The USB port risk analysis enables detailed monitoring and analysis of the activity of USB ports. The data required for the analysis is collected manually from the performance measurement program of the operating system, thereby guaranteeing reliable and accurate results. The process can be automated in the future, which will be explained in more detail in the future description.

Measured values include maximum paging file utilization, disk drive write rate, and CPU and memory utilization. These data are recorded in an object attribute matrix, where the rows show the measured values, these are the objects, while the columns show the elapsed time, these are the attributes. All measurements are made in a two-second time interval, thus ensuring the foundation of a detailed and up-to-date analysis. Based on the raw OAM, we rank and evaluate the various risk factors related to each object as attributes. This enables an objective/optimized exploration of risks. During the analysis, we use the COCO Y0 method, which can be found at https://miau.my-x.hu/myx-free/coco/beker_y0.php.

At the end of the analysis, we perform a validity/authenticity test, which is prepared with the inverse version of the original OAM. The analysis is successful if the inverse of the original results is obtained.

It is important that our data is safe on our own devices, such as computer, laptop, smartphone, tablet. The security of our data is closely related to the protection of our privacy and personal information.

In the online space, we often encounter data theft attempts, hacker attacks or other data security threats. If our data is not secure, it is easily exposed to unauthorized access, which can compromise our identity, financial situation, or even personal relationships.

Losing or damaging our data can cause many inconveniences, be it work, personal documents, photos or other important files.

The protection of our data is not only important from the point of view of our privacy, but also from a financial point of view. Unauthorized access to our financial data (banking information, credit card data, etc.) can pose a significant risk to our financial stability.

If we also store data for business or professional purposes on our computer, their security can be vital for our business or workplace. In case of data loss or data theft, it can significantly affect not only individual work, but also the operation of the company.

Keeping our data safe on our own computer is extremely important not only from a personal, but also from a financial, business and legal point of view.

3. Introduction

3.1. Goals

We store a lot of personal information on computers, such as banking information, health information, personal messages, documents, passwords, etc. The leakage or loss of this data can have serious consequences, such as identity theft or financial fraud. My goal is to keep your data safe and to protect the user from possible data theft, data loss and possible data abuse. Prevention of data loss, protection of personal data. The goal is to perform an analysis of the aggregated risks of an object with a procedure suitable for automation, and a solution to minimize the chance/risk of possible data theft.

3.2. Task

The raw data (e.g. maximum unused page file, disk drive write rate, free space, etc.) is currently extracted manually from the performance monitor on the Windows 11 operating system. Among other things, the long-term goal is the automation of this data collection process and the development of a software for risk estimation. The performance monitor built into the operating system is run by pressing the Win+R key combination and entering the "perfmon.msc" command in the run. Individual measurement aspects can be specified in the performance monitor, e.g.:

1. The maximum utilization of the paging file measured as a percentage .
2. Paging file utilization measured as a percentage
3. Disk drive write rate measured as a percentage.
4. Disk drive utilization measured as a percentage.
5. Disk drive read rate measured as a percentage..
6. Free space measured as a percentage.
7. Pre-recorded memory utilization measured as a percentage.
8. The percentage of processor usage in user mode.
9. Processor utilization measured as a percentage.

Paging file: Also known as virtual memory, which allows the computer to perceive as if there is more physical memory than is available. It helps optimize memory usage and allows your computer to use resources more efficiently.

Disk drive write rate*:* The hard disk write rate is the amount of data that is written to the hard disk during a given time-period, usually expressed per second or per minute. This data transfer rate shows how fast the hard drive can handle write operations. The importance of the write ratio of the hard disk occurs during the storage, copying and processing of data. The faster the write rate, the faster the hard drive can record data. The write rate of the hard disk can be affected by various factors, such as the physical properties of the hard disk (e.g. rotation speed, data transfer rate), the connection interface (e.g. SATA, NVMe), the compression ratio of the hard disk, and the load of other processes and applications running in the system. In general, fast hard drives such as SSDs provide better write rates than conventional hard drives.

Disk drive utilization: This metric shows the fraction of elapsed time in which the selected disk is serving read or write requests.

Disk drive read rate: The read rate of a disk drive indicates the speed of the drive.

Free place on hard disk: Defines the usable free space of the storage disk.

Pre-recorded memory utilization*:* The utilization of the reserved memory shows how actively the system uses these caches to store and access data.

The percentage of CPU usage in user mode: refers to the time ratio between the tasks performed by the operating system or other system software and the processes started by the user.

Processor utilization: The amount of processor power required by the system or applications. This is usually the ratio of the work done by the processor to the total available capacity. The unit of measure for processor utilization is the percentage, which shows that the processor is currently active in a given proportion of time, i.e. how much is its load compared to the maximum available performance.

3.3 Target groups

- Private individuals for home use for data protection.
- Companies where the security of the data is of interest/extremely important, and huge damages can occur as a result of a quasi-data leak.

3.4 Usefulness

Data protection is very important for every private or legal person in digitalization and the online space. Tremendous damage can be caused if privately owned private and confidential data falls into unauthorized hands. Data protection is the basis for preventing identity theft, financial fraud and other crimes. Data protection is not only about protecting against unauthorized access, but also about preventing data loss or corruption, which can lead to the loss or unavailability of important information. In a business or organizational environment, the protection of business secrets, corporate strategies, product plans and other confidential information is essential for maintaining individual or organizational competitiveness. Keeping our data secure is key to individual and organizational security, credibility and competitiveness.

4. Literary/ own history

"In 19961, the USB (Universal Serial Bus) port appeared on the market. A USB port is an interface that allows devices to be connected to a computer or other device. USB ports are widely used because they are flexible and suitable for connecting a variety of devices. The connectors can be grouped in the form of USB standards.

It's usually found as a flat, wide, and flat-shaped opening on the side or back of a computer, laptop, or other device. They can be blue, black or white and come in a variety of variants including USB 1.0, USB 2.0, USB 3.0 and USB-C ports. Usually, USB ports act as input or output interfaces. Input ports allow data and power to be input to a device, such as a USB mouse or keyboard. Output ports allow data and power to be output, such as a USB printer or speaker.

Thanks to technological progress, USB ports provide increasingly faster speeds and greater data transfer capacity. For example, USB 3.0 ports offer faster data transfer speeds (up to 5 Gbps), while USB-C ports allow power and data transfer via the same cable. USB is a technology that allows you to connect devices to your computer or other devices using a cable. A wide range of devices with such USB ports can be connected, and the use of USB can be used for many purposes, the most important of which are:"

1. **Data storage:** USB drives have a large data storage capacity, allowing data to be transferred and stored. USB drives provide a convenient and portable data storage solution.
2. **Connecting Peripherals:** USB ports allow you to connect peripherals such as mouse, keyboard, printer, webcam, speaker or microphone.
3. **Charging mobile devices:** USB ports allow you to charge mobile phones, tablets and other portable devices. By connecting the USB cable, devices can be charged from multiple sources, such as a computer, a portable charger, or a car's USB port.
4. **Data transfer**: USB ports enable fast data transfer between different devices. For example, data can be transferred from the computer to the USB drive or from the mobile phone to the computer.

5. **Network connection:** USB Ethernet adapters allow the use of USB ports for network connection. With such adapters, it is possible to connect the computer to the Internet or other network devices.

[1] Izsáki Gábor. (2023.03.22.) usb-portok-es-szabvanyok html. Download: 2024.04.05. Source: https://laptopguru.hu/laptopgurumagazin/usb-portok-es-szabvanyok/

The USB port is suitable for connecting many devices.

4.1. VID/ PID identifier

Abbreviations for Vendor ID and Product ID. The devices are provided with the VID and PID identifiers by the manufacturers. These are unique codes for USB devices. Based on this, the operating system identifies the device and downloads the corresponding driver.

4.2. OAM

An object attribute matrix is a structure intended to support the determination of similarity between objects based on their attributes. OAM is nothing more than a kind of learning pattern. An "object" can be, for example, a document, an image, a product or any other entity that has attributes, i.e. characteristics, properties. In an object attribute matrix, objects are represented by rows and attributes are represented by columns, where the values of each cell can be characteristics of a given attribute of that object, such as binary (presence or absence), numeric, or categorical values

4.3. The OAM characterization with ChatGPT

Question: *Please describe an object attribute matrix risk analysis in IT.*

*„**ChatGPT**: Object attribute matrix risk analysis in IT is a method often used in software development projects to identify and manage potential risks between objects (classes) and their attributes (properties).*

This method helps to identify and prioritize different risks that can affect the software development process or the finished software. In this case, the attribute matrix is constructed in such a way that the classes or objects are compared with each other in terms of risks.

In the attribute matrix, the classes or objects can be the rows, while the risk factors can be the columns. Risk factors are attributes or properties that may represent potential risks, such as complexity, missing documentation, malfunctioning, etc.

For example, when a software development team starts a new project, the attributes might be:

Complexity: How complex is the class or object?

Probability of errors: How likely are errors to occur on the given object?

Testability: How easy or difficult is the object to test?

Missing Documentation: What documentation is missing for the class or object?

Number of dependencies: How many other classes or objects depend on that object?

For example, a matrix of this type might look like this:

Classes	*Komplexity*	*Error-probability*	*Testing*	*Lack of documentation*	*Number of dependencies*
Class1	*High*	*High*	*Heavy*	*Low*	*8*
Class2	*Low*	*Medium*	*Easy*	*High*	*3*
Class3	*Medium*	*High*	*Heavy*	*Low*	*6*

In this case, the matrix helps to identify which classes or objects have the greatest risk factors and can therefore help the team to pay special attention to these elements during the project. In this way, you can promote more effective risk management and a more successful closing of the project. "

I was wondering how AI-artificial intelligence would think and describe the concept of OAM. From the answer, I conclude that the AI would analyse an object attribute matrix with the basic operations (e.g. mode, median, correlation, standard deviation, etc.). Does it not focus on an analytical model, i.e. can everyone be the same differently? "In the context of similarity analysis2, this is the Y0-MIN model, where min means that the goal of optimization is to minimize some aggregate of estimates and deviations from the consequence variable (Y0), which is fictitious and for all objects, has a constant value (as opposed to the Y0_MAX analysis, in which the goal is the largest possible production of a summarized fact-estimate difference, i.e. classic discrimination, grouping, classification)."

[2] Pető István – MYX Team- Hasonlóságelemzés COCO használatával – Oktatási segédanyag (2013.08.24.) 36. dia https://miau.my-x.hu/miau/189/coco_demo.pdf, (last download: 2024.04.05.)

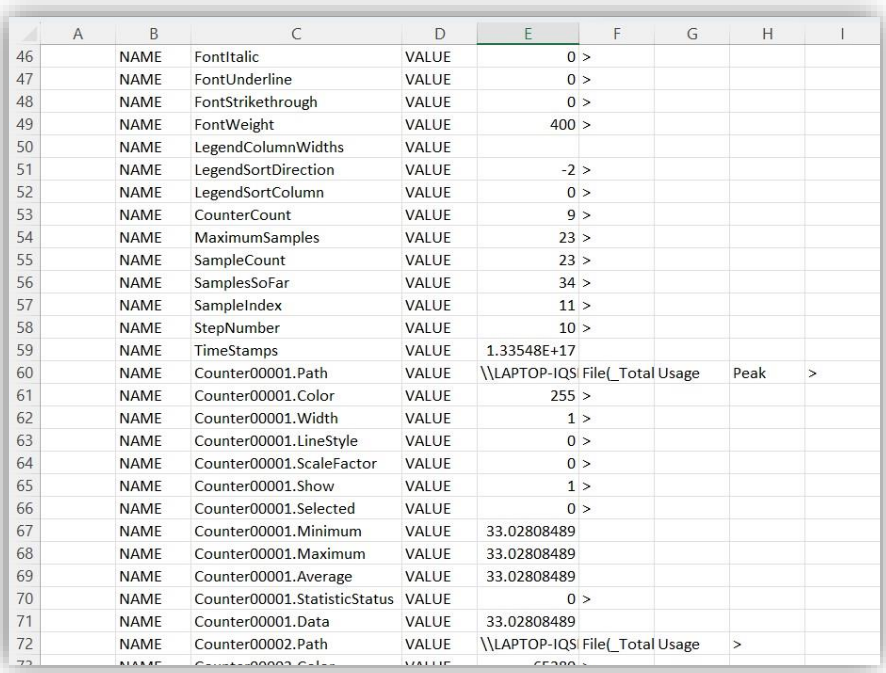
5. Analysis

I collect the data manually, but the goal is to automate it so that the data is displayed to the user in real time. It was already mentioned in the "task" paragraph in my thesis, I extract the data using the performance monitoring application built into the operating system called "perfmon.msc" by pressing the WIN+R keys.

Measurement data are recorded in two-second time intervals. This time interval can be set as desired in the specification of individual aspects.

In my analysis, I recorded 10 measurements to illustrate the task.

After copying the data, I arrange the raw data in the appropriate format in the xlsx table. I convert the text format from text to columns, so the measured data can be copied and become more transparent. I copy the measured parameters into an XLSX table and sort them manually, then create an object attribute matrix to start the analysis. (OAM)



	A	B	C	D	E	F	G	H	I
46		NAME	FontItalic	VALUE	0	>			
47		NAME	FontUnderline	VALUE	0	>			
48		NAME	FontStrikethrough	VALUE	0	>			
49		NAME	FontWeight	VALUE	400	>			
50		NAME	LegendColumnWidths	VALUE					
51		NAME	LegendSortDirection	VALUE	-2	>			
52		NAME	LegendSortColumn	VALUE	0	>			
53		NAME	CounterCount	VALUE	9	>			
54		NAME	MaximumSamples	VALUE	23	>			
55		NAME	SampleCount	VALUE	23	>			
56		NAME	SamplesSoFar	VALUE	34	>			
57		NAME	SampleIndex	VALUE	11	>			
58		NAME	StepNumber	VALUE	10	>			
59		NAME	TimeStamps	VALUE	1.33548E+17				
60		NAME	Counter00001.Path	VALUE	\\LAPTOP-IQS	File(_Total	Usage	Peak	>
61		NAME	Counter00001.Color	VALUE	255	>			
62		NAME	Counter00001.Width	VALUE	1	>			
63		NAME	Counter00001.LineStyle	VALUE	0	>			
64		NAME	Counter00001.ScaleFactor	VALUE	0	>			
65		NAME	Counter00001.Show	VALUE	1	>			
66		NAME	Counter00001.Selected	VALUE	0	>			
67		NAME	Counter00001.Minimum	VALUE	33.02808489				
68		NAME	Counter00001.Maximum	VALUE	33.02808489				
69		NAME	Counter00001.Average	VALUE	33.02808489				
70		NAME	Counter00001.StatisticStatus	VALUE	0	>			
71		NAME	Counter00001.Data	VALUE	33.02808489				
72		NAME	Counter00002.Path	VALUE	\\LAPTOP-IQS	File(_Total	Usage	>	

1. figure: The raw data from text to column

Source: https://miau.my-x.hu/bprof/2024/tavasz/Rapid_usb_monitor_oam.xlsx, „Raw0" page

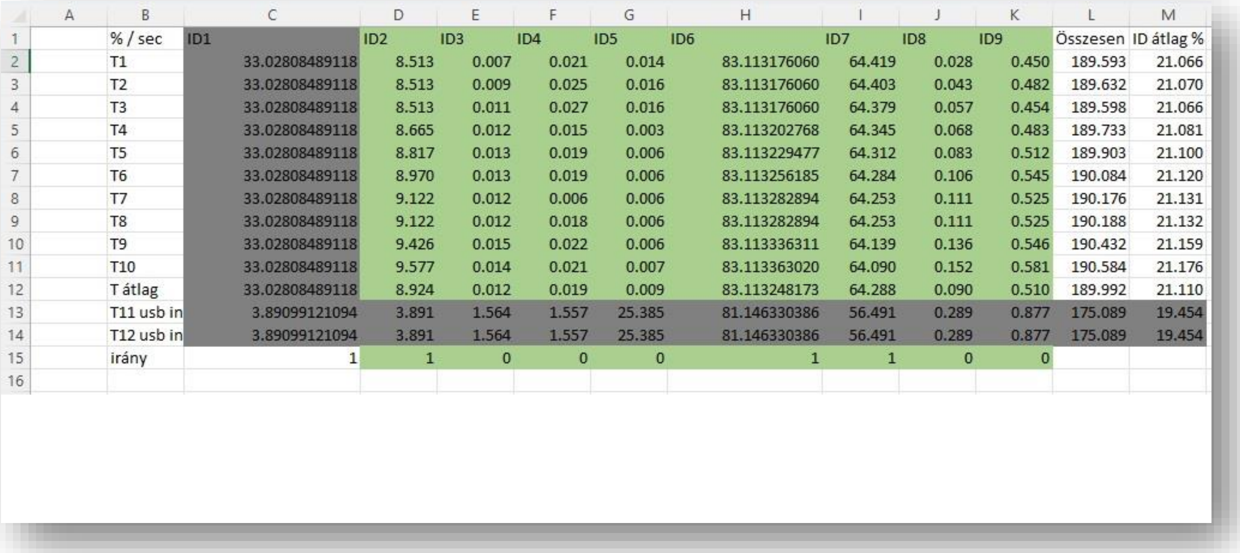
The rows contain the objects and the columns the attributes.

5.1. Objects

The comparable things and phenomena. In this case, the objects are the measured time intervals (T1), i.e. the lines, the unit of measure of which is time (sec., i.e. secundum)

5.2. Attributes

A parameter, pointer, index number that is associated with the object and has a unit of measure. The attributes "ID" are the measured parameters, the unit of measure is percentage (%) (paging file, disk drive, etc.), i.e. the columns.



	A	B	C	D	E	F	G	H	I	J	K	L	M
1		% / sec	ID1	ID2	ID3	ID4	ID5	ID6	ID7	ID8	ID9	Összesen	ID átlag %
2		T1	33.02808489118	8.513	0.007	0.021	0.014	83.113176060	64.419	0.028	0.450	189.593	21.066
3		T2	33.02808489118	8.513	0.009	0.025	0.016	83.113176060	64.403	0.043	0.482	189.632	21.070
4		T3	33.02808489118	8.513	0.011	0.027	0.016	83.113176060	64.379	0.057	0.454	189.598	21.066
5		T4	33.02808489118	8.665	0.012	0.015	0.003	83.113202768	64.345	0.068	0.483	189.733	21.081
6		T5	33.02808489118	8.817	0.013	0.019	0.006	83.113229477	64.312	0.083	0.512	189.903	21.100
7		T6	33.02808489118	8.970	0.013	0.019	0.006	83.113256185	64.284	0.106	0.545	190.084	21.120
8		T7	33.02808489118	9.122	0.012	0.006	0.006	83.113282894	64.253	0.111	0.525	190.176	21.131
9		T8	33.02808489118	9.122	0.012	0.018	0.006	83.113282894	64.253	0.111	0.525	190.188	21.132
10		T9	33.02808489118	9.426	0.015	0.022	0.006	83.113336311	64.139	0.136	0.546	190.432	21.159
11		T10	33.02808489118	9.577	0.014	0.021	0.007	83.113363020	64.090	0.152	0.581	190.584	21.176
12		T átlag	33.02808489118	8.924	0.012	0.019	0.009	83.113248173	64.288	0.090	0.510	189.992	21.110
13		T11 usb in	3.89099121094	3.891	1.564	1.557	25.385	81.146330386	56.491	0.289	0.877	175.089	19.454
14		T12 usb in	3.89099121094	3.891	1.564	1.557	25.385	81.146330386	56.491	0.289	0.877	175.089	19.454
15		irány	1	1	0	0	0	1	1	0	0		
16													

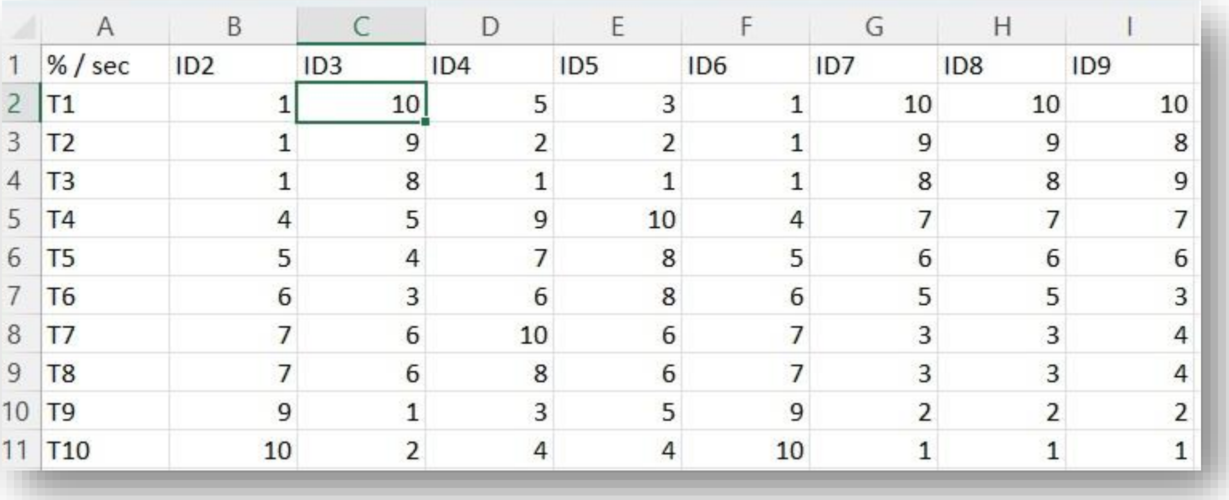
2. figure: Sorting the raw data into an Object Attribute Matrix. (Rows: object(sec), column: attribute (%)

Source: https://miau.my-x.hu/bprof/2024/tavasz/Rapid_usb_monitor_oam.xlsx, „OAM Transp." page

We do not consider identical data as part of the analysis, so the ranking is created by ignoring that data. We specify that if there is a positive risk and the higher the value, the greater the risk, and if there is a negative risk, then the lower the value, the greater the risk. (ie the benchmark)

5.3. Ranking

Ranking is the relative ordering of objects or alternatives based on attributes in a given matrix. In risk analysis, this is important because it allows us to identify and prioritize objects or alternatives that carry the highest or lowest risk based on given attributes. Prioritization helps us understand more easily which objects or alternatives need to be addressed and which are most important for risk management or decision making.



	A	B	C	D	E	F	G	H	I
1	% / sec	ID2	ID3	ID4	ID5	ID6	ID7	ID8	ID9
2	T1	1	10	5	3	1	10	10	10
3	T2	1	9	2	2	1	9	9	8
4	T3	1	8	1	1	1	8	8	9
5	T4	4	5	9	10	4	7	7	7
6	T5	5	4	7	8	5	6	6	6
7	T6	6	3	6	8	6	5	5	3
8	T7	7	6	10	6	7	3	3	4
9	T8	7	6	8	6	7	3	3	4
10	T9	9	1	3	5	9	2	2	2
11	T10	10	2	4	4	10	1	1	1

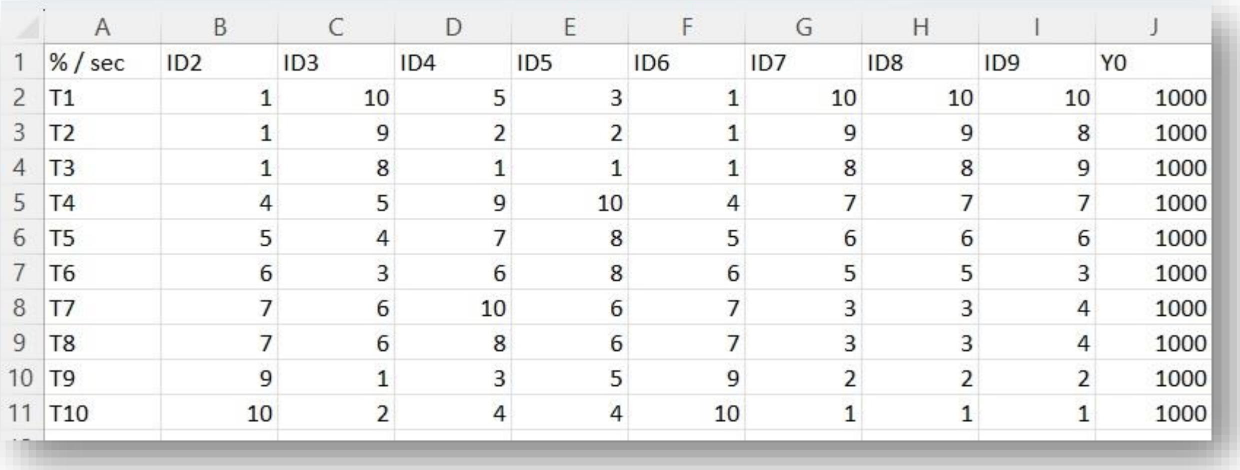
3. figure: Ranking (Rows: object (sec), column: attribute (row number)

Source: https://miau.my-x.hu/bprof/2024/tavasz/Rapid_usb_monitor_oam.xlsx,

„OAM rank 2" page

During the analysis, we use the COCO method and this is done with the COCO Y0 online model. After ranking, we add an identical value Y0 to this object.

Based on this, the COCO model performs calculations and provides an estimate for each object. We copy our table without column and row headers into the COCO Y0 model and start the analysis by clicking the "run" button.

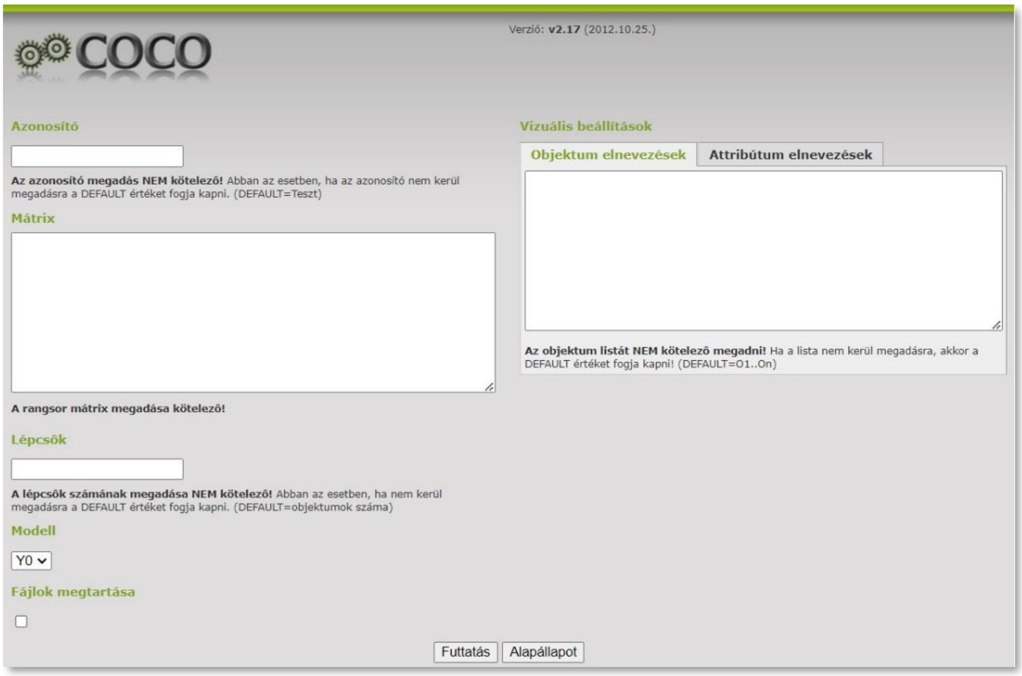


	A	B	C	D	E	F	G	H	I	J
1	% / sec	ID2	ID3	ID4	ID5	ID6	ID7	ID8	ID9	Y0
2	T1	1	10	5	3	1	10	10	10	1000
3	T2	1	9	2	2	1	9	9	8	1000
4	T3	1	8	1	1	1	8	8	9	1000
5	T4	4	5	9	10	4	7	7	7	1000
6	T5	5	4	7	8	5	6	6	6	1000
7	T6	6	3	6	8	6	5	5	3	1000
8	T7	7	6	10	6	7	3	3	4	1000
9	T8	7	6	8	6	7	3	3	4	1000
10	T9	9	1	3	5	9	2	2	2	1000
11	T10	10	2	4	4	10	1	1	1	1000

4. figure: Rank and add Y0 value (Rows: object(sec), column: attribute (rownumber)

Source: https://miau.my-x.hu/bprof/2024/tavasz/Rapid_usb_monitor_oam.xlsx,

„OAM rank 2" page



COCO

Verzió: **v2.17** (2012.10.25.)

Azonosító

Az azonosító megadás NEM kötelező! Abban az esetben, ha az azonosító nem kerül megadásra a DEFAULT értéket fogja kapni. (DEFAULT=Teszt)

Mátrix

A rangsor mátrix megadása kötelező!

Lépcsők

A lépcsők számának megadása NEM kötelező! Abban az esetben, ha nem kerül megadásra a DEFAULT értéket fogja kapni. (DEFAULT=objektumok száma)

Modell

Y0

Fájlok megtartása

☐

Vizuális beállítások

Az objektum listát NEM kötelező megadni! Ha a lista nem kerül megadásra, akkor a DEFAULT értéket fogja kapni! (DEFAULT=O1..On)

5. figure: A COCO Y0 model- input surface

Source: https://miau.my-x.hu/myx-free/coco/beker_y0.php

The[3] COCO analysis (component-based object comparison for objectivity)

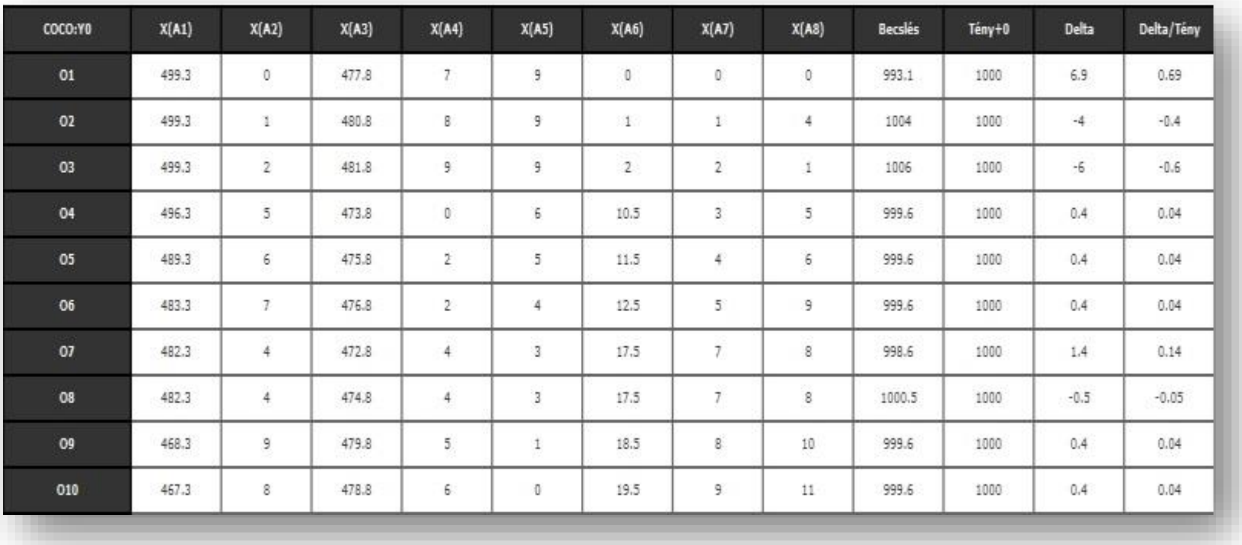
It shows that the examined objects (countries, companies, projects, products, tenders, etc.) are under- or over-valued compared to each other based on their characteristics included in the study.

Undervaluation and overvaluation are examined from the point of view of a characteristic with a privileged role, the dependent variable of the model (Y-variable).

During the construction of the model, we get a Y-component for each property of each object, and by summing them row by row, the estimated Y is created for each object.

The preparation of the basic version of the model contains a subjective element at two points: in the selection of the factors and in specifying the direction of the ranking.

[3] Pető István – MYX Team- Hasonlóságelemzés COCO használatával – Oktatási segédanyag (2013.08.24.) 12. dia https://miau.my-x.hu/miau/189/coco_demo.pdf, (utolsó letöltés: 2024.04.05.)



COCO:Y0	X(A1)	X(A2)	X(A3)	X(A4)	X(A5)	X(A6)	X(A7)	X(A8)	Becslés	Tény+0	Delta	Delta/Tény
O1	499.3	0	477.8	7	9	0	0	0	993.1	1000	6.9	0.69
O2	499.3	1	480.8	8	9	1	1	4	1004	1000	-4	-0.4
O3	499.3	2	481.8	9	9	2	2	1	1006	1000	-6	-0.6
O4	496.3	5	473.8	0	6	10.5	3	5	999.6	1000	0.4	0.04
O5	489.3	6	475.8	2	5	11.5	4	6	999.6	1000	0.4	0.04
O6	483.3	7	476.8	2	4	12.5	5	9	999.6	1000	0.4	0.04
O7	482.3	4	472.8	4	3	17.5	7	8	998.6	1000	1.4	0.14
O8	482.3	4	474.8	4	3	17.5	7	8	1000.5	1000	-0.5	-0.05
O9	468.3	9	479.8	5	1	18.5	8	10	999.6	1000	0.4	0.04
O10	467.3	8	478.8	6	0	19.5	9	11	999.6	1000	0.4	0.04

6.figure: A COCO Y0 model calculation

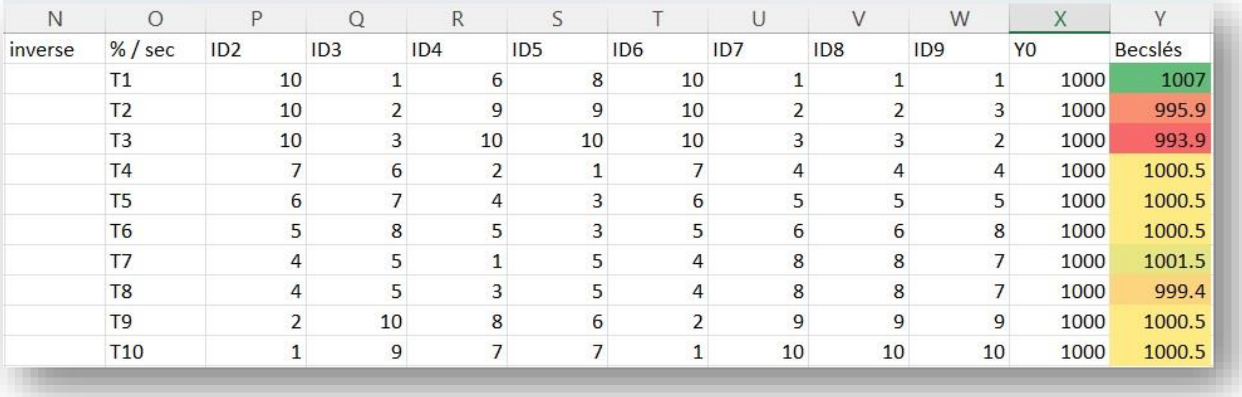
Source: https://miau.my-x.hu/bprof/2024/tavasz/Rapid_usb_monitor_oam.xlsx, „OAM Transp." page

From the returned analysis, we assign the estimate "row" to the existing ranked OAM and we can see which elements are different and involve risk.

[4]In order for the result obtained by COCO to be considered credible, we create an "inverse" ranking OAM. This is the opposite direction from the original OAM. If the result obtained when running the "inverse" is opposite to the original results, then it can be considered authentic. "Essentially, we examine this by comparing the sign of the delta (difference between estimate and fact) values. "

---

[4] Pető István – MYX Team- Hasonlóságelemzés COCO használatával – Oktatási segédanyag (2013.08.24.) 36. dia https://miau.my-x.hu/miau/189/coco_demo.pdf, (utolsó letöltés: 2024.04.05.)

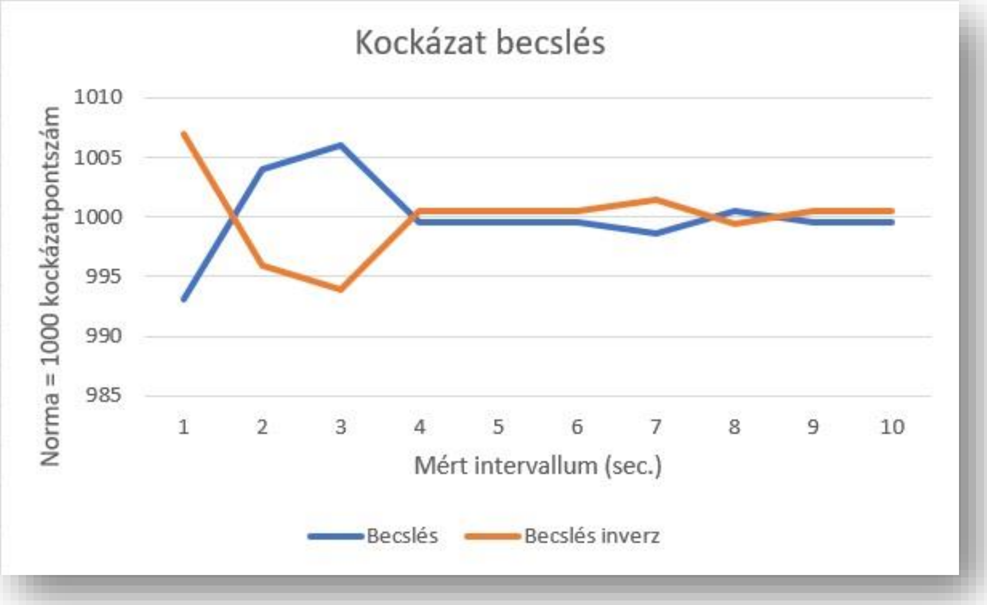


N	O	P	Q	R	S	T	U	V	W	X	Y
inverse	% / sec	ID2	ID3	ID4	ID5	ID6	ID7	ID8	ID9	Y0	Becslés
	T1	10	1	6	8	10	1	1	1	1000	1007
	T2	10	2	9	9	10	2	2	3	1000	995.9
	T3	10	3	10	10	10	3	3	2	1000	993.9
	T4	7	6	2	1	7	4	4	4	1000	1000.5
	T5	6	7	4	3	6	5	5	5	1000	1000.5
	T6	5	8	5	3	5	6	6	8	1000	1000.5
	T7	4	5	1	5	4	8	8	7	1000	1001.5
	T8	4	5	3	5	4	8	8	7	1000	999.4
	T9	2	10	8	6	2	9	9	9	1000	1000.5
	T10	1	9	7	7	1	10	10	10	1000	1000.5

7.figure: *Completed with an estimate evaluated by inverse OAM and the COCO Y0 model. (Rows: object(sec), column: attribute (inverse ranking number: ID2-9, risk score Y0 and estimate)*

Source: https://miau.my-x.hu/bprof/2024/tavasz/Rapid_usb_monitor_oam.xlsx,

„OAM rank 2" page



8.figure: *Risk estimation statement (Blue – Estimation direct, Orange – Estimation inverse, Y: risk index values, X: time)*

Source: https://miau.my-x.hu/bprof/2024/tavasz/Rapid_usb_monitor_oam.xlsx,

„OAM rank 2" page

6. Discussion

You may be wondering why we use this method to check a USB flash drive/device. Different antivirus programs search for files with suspicious extensions from a specific database. However, lines of code written in a programming language are not checked. The identification of USB devices is checked by the operating system (cf. vid/pid identifier) in order to install the correct driver for the given device. However, this can be influenced and is not a sure control method.

7. Conclusions

When sorting raw data into OAM, it can be trivial that the data is similar and identical with minor differences. However, running the analysis well simulates which periods can be risky, i.e. which are the rows that differ from the benchmark. So, the higher the value, the higher the risk, and the lower the value, the higher the risk. Based on this modelling, it is possible to check the activities running in the background on the computer even if a device is connected to our device.

8. Vision

The modelling illustrated in the thesis makes it possible to monitor risky elements with the analysis. The future is the automation of the presented algorithm and the development of an independent software for the security of our data.

9. Attachments

9.1. List of abbreviation:

OAM: Objekt Attribute Matrix, learning pattern

USB: (Universal Serial Bus) port. A USB port is an interface that allows devices to be connected to a computer or other device.

CPU: Central Processing Unit –central processing unit also known as processor

COCO: (Component-based object comparison for objectivity) similarity analysis model family

COCO Y0: anti-discrimination calculations ideal search model

SATA: A Serial ATA (Serial Advanced Technology Attachment)

NVMe: NVMe (Non-Volatile Memory Express). A new generation storage device used to store data in computers.

SSD: solid state drive - is a storage device without moving parts that stores data in memory and is equipped with a connection interface similar to hard drives.

PERFMON.MSC: Microsoft Management Console, a tool within Windows that allows you to monitor and analyze system performance.

XLSX: Microsoft Excel format, spreadsheet manager

VID/ PID identifier: Vendor ID és Product ID abbreviation. USB used to identify devices.

9.2. References

Lehrer Zoltán. (2024.03.21.) Rapid_usb_monitor_oam XLSX. Letöltés: 2024.04.07. Forrás: https://miau.my-x.hu/bprof/2024/tavasz/ Rapid_usb_monitor_oam.xlsx

Dr. Pitlik László. (2014. december) My-X Team_A5 fuzet_HU_jav.pdf. Letöltés: 2024.03.12. Forrás: https://miau.my-x.hu/miau/196/My-X%20Team_A5%20fuzet_HU_jav.pdf

Pető István (2014. május) coco_demo.pdf. Letöltés: 2024.03.27. Forrás: https://miau.my-x.hu/miau/189/coco_demo.pdf

Izsáki Gábor. (2023.03.22.) usb-portok-es-szabvanyok html. Letöltés: 2024.04.05. Forrás: https://laptopguru.hu/laptopgurumagazin/usb-portok-es-szabvanyok/

9.3. List of figures

1. figure: *Sorting the raw data from text to column.*

2. figure: *Sorting the raw data into an Object Attribute Matrix. (Rows: object(sec), column: attribute (%)*

3. figure: *Ranking (Rows: object (sec), column: attribute (row)*

4. figure: *Rank and add Y0 value (Rows: object(sec), column: attribute (rownumber)*

5. figure: *A COCO Y0 modell- input side*

6. figure: *A COCO Y0 modell calculation*

7. figure: *Completed with an estimate evaluated by inverse OAM and the COCO Y0 model. (Rows: object(sec), column: attribute (inverse ranking number: ID2-9, risk score Y0 and estimate)*

8. figure: *Risk estimation statement*