ASSESSING THE VULNERABILITY OF A TRANSPORT MANAGEMENT SYSTEM TO CYBER ATTACKS FOR APPLICATION IN THE METHOD OF THE THREE FACTORS

Yoana A. Ivanova

Department of Informatics, New Bulgarian University
e-mail: yivanova@nbu.bg
Bulgaria

Abstract: This paper is considered to be a continuation of a previous publication devoted to assessment of the probability of cyberattacks on Transport Management Systems *(IJITS, № 4, 2018)*. The specificity of the current research is due to assessing the vulnerability of a Traffic Control Centre (TCC) / Transport Management System (TMSs) respectively to internal and external cyberattacks. The simulation results obtained can be used for more accurate qualitative and quantitative risk assessment, as well as a comparative analysis of internal and external impacts.

Key words: vulnerability, probability, risk, transport management, cybersecurity, cyberattacks, modelling, simulation.

1. INTRODUCTION

The main advantage of the applied "method of the three factors" for risk assessment compared to the previously examined expert approach is its greater accuracy because it is based not only on the two factors (P - probability and C - possible damage) but also on vulnerability assessment of the modelled system.

Actually vulnerability refers to a weakness in a computer system that reduces its security posture. Specifically with regard to TMS the most vulnerable components are TCC and the traffic light signalling system. The elements of the traffic lights signalling system are described in detail in a previous article (*IJITS, № 3, 2017*). A cyberattack to the traffic lights signalling system is simulated by changing the duration of the green light.

Exploit refers to vulnerabilities that have publicly available exploit code as of the time of testing. Risk rankings generally follow the standard CVSS (Common Vulnerability Scoring System):

- Vulnerabilities are labelled "Low" severity if they have a CVSS base score of 0.0 -3.9;

- Vulnerabilities are labelled "Medium" if they have a CVSS base score of 4.0 -6.9;
- Vulnerabilities are labelled "High" severity if they have a CVSS base score of 7.0 -8.9;
- Vulnerabilities are labelled "Critical" severity if they have a CVSS base score of 9.0 – 10.0.

Some examples of specific vulnerabilities in critical infrastructure control systems are given as follows: not reliable authentication and/ or data protection between clients and access points; usage of shared passwords and user accounts in remote access; non-existing protections or incorrect configured firewalls; no security monitoring or critical monitoring and control paths are unidentified, complicating redundancy or contingency plans [1, 2].

The specificity of the simulation system Riverbed Modeller Academic Edition 17.5 for professional use is the approach for assessment of system vulnerability to cyberattacks by setting the vulnerability as an input parameter. Actually this is one of the main principle difference between the method of simulation modelling and other methods for detecting vulnerabilities. The comparative analysis between these methods is needed to highlight the advantages of the simulation modelling as a reliable and innovative method which reduces costs.

For example penetration testing aims to verify the security of the system and in particular to detect potential vulnerabilities in security systems to an external hacking attempt by attacking them in the same way as a potential hacker would. The full process of penetration testing is executed in seven successive phases (Reengagement, Information gathering, Threat modelling, Vulnerability analysis, Exploitation, Post exploitation, Reporting) [3]. For example in algorithms for detecting web based applications vulnerabilities the condition for vulnerable response is placed after the input parameters and preceded by obtaining URLS list, as well as the execution of SQL Test Case [4].

This means that in the simulation process the vulnerability is already a known parameter during the cyberattack modelling itself because the cyber elements and cyber effects can be selected before the simulation execution. From this perspective simulation modelling is more cost-effective for vulnerability assessment primarily because it saves time and accordingly reduces the duration of the subsequent decision-making process, because the efficiency of a penetration test depends on the time for detecting vulnerabilities.

The empirical part of this paper covers two sections: **Section 2** contains the experiments related to assessment of the system vulnerability of TTC as a main component of TMS using the simulation system Riverbed Modeller Academic Edition 17.5, while **Section 3** is dedicated especially to the risk assessment by "the method of the three factors" using the obtained simulation results.

2. ASSESSMENT OF THE SYSYEM VULNERABILITY BY THE METHOD OF SIMULATION MODELLING

In the first part of this research the author investigates the system vulnerability using the model of TCC which is presented in detail in a previous article (*IJITS, № 2, 2017*). The architecture used in the simulation is realistic because it is based on a real existing TCC developed by Huawei. The connection between the tests performed based on the simulation model of TCC and TMS is that the TCC is the main component of each TMS. The results of simulation modelling are sufficiently reliable and do not need to be compared with results of other methods. The vulnerability values are set sequentially in three scenarios by setting different values of the main input parameter interarrival time T. This simulation model is regarded as the target object of an internal DoS attack.

Table 1, 2 and 3 contain the summary results of all three charts, showing the registered peak levels of "traffic sent" T_S and "traffic received" T_R as functions of T ($T_1 = 2$ [s], $T_2 = 1$ [s] and $T_3 = 0.2$ [s]) at system vulnerability to cyberattacks V from 5 to 100%. The duration of this simulation is divided into six equal intervals of 5 seconds ([1, 5], [5, 10], [10, 15], [15, 20], [20, 25], [25, 30]).

The second part of this research is essentially similar to the first part, but the simulated DoS attack to the TCC is external, because its source is located out of the TCC. The simulation results are presented in Tables 4, 5 and 6.

Table 1

	T1, s											
	R1, s		***R2, s***		***R3, s***		***R4, s***		***R5, s***		***R6, s***	
V, %	T_S,	T_R	T_S	T_R	T_S	T_R	T_S	T_R	T_S	T_R	T_S	T_R
5	3.3	3.3	3.3	3.3	3.3	3.3	6.7	3.3	10	6.7	6.7	3.3
10	3.3	3.3	3.3	3.3	3.3	3.3	6.7	3.3	10	6.7	6.7	3.3
20	3.3	3.3	3.3	3.3	3.3	0	6.7	3.3	10	6.7	6.7	3.3
50	3.3	3.3	3.3	3.3	3.3	0	6.7	3.3	10	6.7	6.7	3.3
80	3.3	3.3	3.3	3.3	3.3	0	6.7	3.3	10	6.7	6.7	3.3
90	3.3	3.3	3.3	3.3	3.3	0	6.7	3.3	10	6.7	6.7	3.3
100	3.3	3.3	3.3	3.3	3.3	0	6.7	3.3	10	6.7	6.7	3.3

Table 2.

	T_2, s											
	R_1, s		R_2, s		R_3, s		R_4, s		R_5, s		R_6, s	
V, %	T_S	T_R	T_S	T_R	T_S	T_R	T_S	T_R	T_S	T_R	T_S	T_R
5	3.3	3.3	3.3	3.3	3.3	3.3	10	3.3	6.7	3.3	6.7	6.7
10	3.3	3.3	3.3	3.3	3.3	3.3	10	3.3	6.7	3.3	6.7	6.7
20	3.3	3.3	3.3	3.3	3.3	3.3	10	3.3	6.7	3.3	6.7	6.7
50	3.3	3.3	3.3	3.3	3.3	3.3	10	3.3	6.7	3.3	6.7	6.7
80	3.3	3.3	3.3	3.3	3.3	3.3	10	3.3	6.7	3.3	6.7	6.7
90	3.3	3.3	3.3	3.3	3.3	3.3	10	3.3	6.7	3.3	6.7	6.7
100	3.3	3.3	3.3	3.3	3.3	3.3	10	3.3	6.7	3.3	6.7	6.7

Table 3

	T_3, s											
	R_1, s		R_2, s		R_3, s		R_4, s		R_5, s		R_6, s	
V, %	T_S	T_R	T_S	T_R	T_S	T_R	T_S	T_R	T_S	T_R	T_S	T_R
5	6.7	6.7	13.5	6.7	13.5	6.7	10	13.5	13.5	6.7	16.7	10
10	6.7	6.7	13.5	6.7	13.5	6.7	13.5	13.5	13.5	6.7	16.7	10
20	6.7	6.7	13.5	6.7	13.5	6.7	13.5	13.5	13.5	6.7	16.7	10
50	6.7	6.7	13.5	6.7	13.5	10	13.5	10	13.5	6.7	16.7	10
80	6.7	6.7	13.5	6.7	13.5	10	13.5	10	13.5	6.7	16.7	10
90	6.7	6.7	13.5	6.7	13.5	10	13.5	13.5	13.5	6.7	16.7	10
100	6.7	6.7	13.5	6.7	13.5	10	13.5	13.5	13.5	6.7	16.7	10

Table 4

	T_1, s											
	R_1, s		R_2, s		R_3, s		R_4, s		R_5, s		R_6, s	
V, %	T_S,	T_R	T_S	T_R	T_S	T_R	T_S	T_R	T_S	T_R	T_S	T_R
5	3.3	3.3	3.3	3.3	3.3	3.3	3.3	3.3	6.7	3.3	3.3	3.3
10	3.3	3.3	3.3	3.3	3.3	3.3	3.3	3.3	6.7	3.3	3.3	3.3
20	3.3	3.3	3.3	3.3	3.3	3.3	3.3	3.3	6.7	3.3	3.3	3.3
50	3.3	3.3	3.3	3.3	3.3	3.3	3.3	3.3	6.7	3.3	3.3	3.3
80	3.3	3.3	3.3	3.3	3.3	3.3	3.3	3.3	6.7	3.3	3.3	3.3
90	3.3	3.3	3.3	3.3	3.3	3.3	3.3	3.3	6.7	3.3	3.3	3.3
100	3.3	3.3	3.3	3.3	3.3	3.3	3.3	3.3	6.7	3.3	3.3	3.3

Table 5.

	T_2, s											
	R_1, s		R_2, s		R_3, s		R_4, s		R_5, s		R_6, s	
V, %	T_S	T_R	T_S	T_R	T_S	T_R	T_S	T_R	T_S	T_R	T_S	T_R
5	6.7	3.3	6.7	3.3	3.3	3.3	6.7	3.3	3.3	3.3	3.3	0
10	6.7	3.3	6.7	3.3	3.3	3.3	6.7	3.3	3.3	3.3	3.3	0
20	6.7	3.3	6.7	3.3	3.3	3.3	6.7	3.3	3.3	3.3	3.3	0
50	6.7	3.3	6.7	3.3	3.3	3.3	6.7	3.3	3.3	3.3	3.3	0
80	6.7	3.3	6.7	3.3	3.3	3.3	6.7	3.3	3.3	3.3	3.3	0
90	6.7	3.3	6.7	3.3	3.3	3.3	6.7	3.3	3.3	3.3	3.3	0
100	6.7	3.3	6.7	3.3	3.3	3.3	6.7	3.3	3.3	3.3	3.3	0

Table 6

	T_3, s											
	R_1, s		R_2, s		R_3, s		R_4, s		R_5, s		R_6, s	
V, %	T_S	T_R	T_S	T_R	T_S	T_R	T_S	T_R	T_S	T_R	T_S	T_R
5	16	6.7	10	6.7	7	3.3	13.1	10	13.1	10	20	10
10	16	6.7	10	6.7	7	3.3	13.1	10	13.1	10	20	10
20	16	6.7	10	6.7	7	3.3	13.1	10	13.1	10	20	10
50	16	6.7	10	6.7	7	3.3	13.1	10	13.1	10	20	10

80	16	6.7	10	6.7	7	3.3	13.1	10	13.1	10	20	10
90	16	6.7	10	6.7	7	3.3	13.1	10	13.1	10	20	10
100	16	6.7	10	6.7	7	3.3	13.1	10	13.1	10	20	10

Table 7 contains the number of the adverse events (m) as a result of changing the system vulnerability (V) for three selected scenarios under the impact of an internal and external DoS attack on the TCC. The number of all events for each scenario is n = 6, because the duration of the simulation is divided into 6 equal intervals of 5 seconds. Consequently, in this case the probability is calculated as a ratio of the number of adverse events (m) to the total number of events (n). The author makes the assumption that the adverse events are expressed in anomalous values of "traffic sent" ($T_{S, max}$) and "traffic received" ($T_{R, max}$).

The column diagram in Figure 1 shows the dependence between the probability P and the vulnerability V for Scenario 10 respectively under the impact of an internal and external cyberattack ($P_{internal}$ and $P_{external}$).

Table 7

			Internal cyberattack		***External cyberattack***	
V, %	***Scenario***	***T, s***	***m***	***P***	***m***	***P***
5	1	2	3	0.5	1	0.17
	5	0.2	2	0.33	4	0.67
	10	0.02	5	0.83	6	1
10	1	2	3	0.5	1	0.17
	5	0.2	2	0.33	4	0.67
	10	0.02	4	0.67	6	1
20	1	2	4	0.67	1	0.17
	5	0.2	2	0.33	4	0.67
	10	0.02	4	0.67	6	1
50	1	2	4	0.67	1	0.17
	5	0.2	2	0.33	4	0.67
	10	0.02	5	0.83	6	1
80	1	2	4	0.67	1	0.17
	5	0.2	2	0.33	4	0.67
	10	0.02	5	0.83	6	1
90	1	2	4	0.67	1	0.17
	5	0.2	2	0.33	4	0.67
	10	0.02	4	0.67	6	1
100	1	2	4	0.67	1	0.17
	5	0.2	2	0.33	4	0.67
	10	0.02	4	0.67	6	1

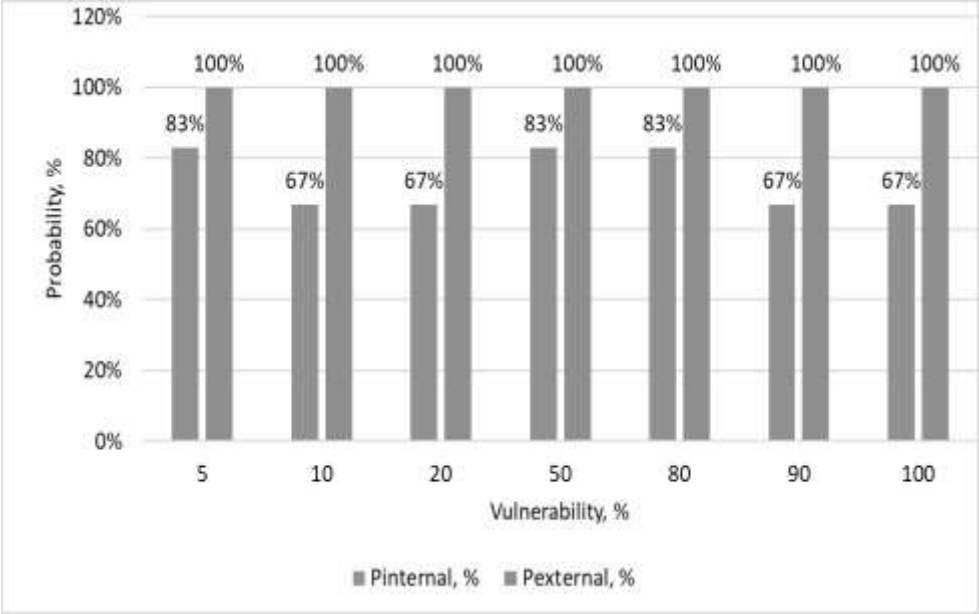

Fig. 1. Graphical interpretation of P = f(V) for TCC/TMSs.

3. RISK ASSESSMENT BY THE METHOD OF THE THREE FACTORS

Whereas according to the expert method the risk R can be presented as a function of P [R = f(P)] by a probability distribution, the method of the three factors includes another very meaningful factor – vulnerability V. There are different formulations of this method in terms of parameters involved in the formula.

Risk can be presented conceptually with a basic equation $\boldsymbol{R = H*V*E}$, where H is hazard, V – vulnerability and E – exposure in the sense of elements at risk (people or assets). In this case the risk is defined as the probability of harmful consequences, or expected losses (deaths, injuries, property, livelihoods, economic activity disrupted or environment damaged) resulting from interactions between various hazards and vulnerable conditions [5].

The preferred formulation by the author is $\boldsymbol{R = P*C*V}$ [6], where the negative consequences C are calculated by a conditional expert determination based on the number of the adverse events. For example, C is maximum of 1 (100 %) if m = n = 6. When m = 1 and n = 6, C is calculated as a ratio of 1 to 6 and its value is respectively 2, 3, 4 or 5 times more if m = 2, 3, 4, 5. The simulation results of the quantitative risk assessment using this method are presented in Table 8.

It is acceptable according to the specificity of a research instead of C to be used hazard H.

Table 8

			Internal cyberattack			***External cyberattack***		
V, %	***Scenario***	***T [s]***	***P***	***C***	***R***	***P***	***C***	***R***
5	1	2	0.5	0.5	0.012	0.17	0.17	0.001
	5	0.2	0.33	0.33	0.005	0.67	0.67	0.022
	10	0.02	0.83	0.83	0.034	1	1	0.05
10	1	2	0.5	0.5	0.025	0.17	0.17	0.003
	5	0.2	0.33	0.33	0.010	0.67	0.67	0.045
	10	0.02	0.67	0.67	0.045	1	1	0.100
20	1	2	0.67	0.67	0.090	0.17	0.17	0.006
	5	0.2	0.33	0.33	0.022	0.67	0.67	0.090
	10	0.02	0.67	0.67	0.090	1	1	0.200
50	1	2	0.67	0.67	0.224	0.17	0.17	0.014
	5	0.2	0.33	0.33	0.054	0.67	0.67	0.224
	10	0.02	0.83	0.83	0.344	1	1	0.500
80	1	2	0.67	0.67	0.360	0.17	0.17	0.023
	5	0.2	0.33	0.33	0.087	0.67	0.67	0.360
	10	0.02	0.83	0.83	0.551	1	1	0.800
90	1	2	0.67	0.67	0.404	0.17	0.17	0.026
	5	0.2	0.33	0.33	0.098	0.67	0.67	0.404
	10	0.02	0.67	0.67	0.404	1	1	0.900
100	1	2	0.67	0.67	0.449	0.17	0.17	0.028
	5	0.2	0.33	0.33	0.109	0.67	0.67	0.449
	10	0.02	0.67	0.67	0.449	1	1	1

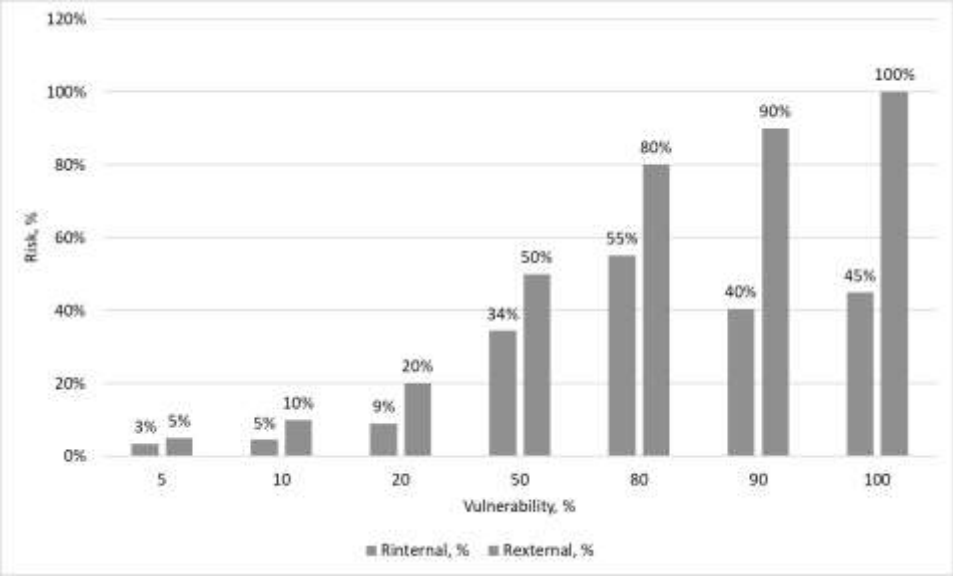

Fig. 2. Graphical interpretation of R = f(V) for TCC/TMSs.

In this case the summary evaluation based on the graphical and tabular results shown in Figure 2 and Table 8 is that the generated simulation results are reliable and suitable for risk assessment and analysis. The regularity of these results is visible because the risk levels are highest when the system vulnerability exceeds the critical 50 %. Another important conclusion is that the risk is greater under the impact of an external cyberattack.

Actually the main difference between the internal and external cyberattack is in the location of the attacker. In the simulation system the external cyberattack is simulated by an attacker placed outside the TCC. When the cyberattack is internal the attacker is placed inside the TCC. In Riverbed Academic Edition 17.5 the attacker is presented by a workstation with specific settings. In particular a DoS attack has a negative impact on the computational resources of the infected server and causes exhaustion of the bandwidth of the Internet connection channel.

4. CONCLUSION

Cybersecurity defines the degree of influence of information or physical environment on a system. In case when transition of system in an unsafe state can be caused by attack via open or partially open cyber space a concept “cyber safety” can be used [7]. Cyber-security failures can increase risks and negative consequences, because invulnerable systems do not exist in practice.

The reducing risk can be achieved by more effective vulnerability analysis and especially identifying cyber threats and weak points in the systems on time by performing a regular comprehensive assessment, monitoring and prevention. In particular, reducing common vulnerabilities in critical infrastructure control systems

is possible using modern TCP/IP systems, as well as complex means of protection combining firewalls, VPN, antivirus software and etc.

This research can be continued by conducting new series of experiments for strengthening the protection of the TCC and studying the specific vulnerabilities of the connected devices and elements. Their level of effectiveness can be evaluated by the expert in simulation environment using the presented approach.

REFERENCES

[1] Underwood K., Laliberte S., Retrum A., Armknecht R., Walter M., Stewart T, 2018 Security Threat Report, Assessing Nine Years of Cyber Security Vulnerabilities and Exploits, 2018, https://www.protiviti.com/sites/default/files/united_states/insights/2018-security-threat-report_protiviti.pdf.

[2] Stamp, J., Dillinger J., Young W, DePoy J, Common Vulnerabilities in Critical Infrastructure control Systems, Sandia National Laboratories, Albuquerque, United States, 2003, https://www.smartgrid.gov/files/Common_Vulnerabilities_in_Critical_Infrastructure_Control_Sy_200310.pdf.

[3] Weidman, G., *Penetration Testing: a Hands-on Introduction to Hacking*, No Starch Press Inc., San Francisco, 2014, pp. 2-6.

[4] Karumba M., Ruhiu S., Moturi C., A Hybrid Algorithm for Detecting Web Based Applications Vulnerabilities, *American Journal of Computing Research Repository*, 1 (vol. 4), 2016, pp. 15-20.

[5] Van Westen C. J., "Methods for Risk Assessment", CHARIM Carribean Handbook on Risk Information Management, University of Twente, 2016, http://www.charim.net/methodology/55.

[6] Lewis T. G., Critical infrastructure protection in homeland security, defending a networked nation, Hoboken, New Jersey: John Wiley & Sons, 2015, https://www.worldcat.org/title/critical-infrastructure-protection-in-homeland-security-defending-a-networked-nation/oclc/910911932&referer=brief_results.

[7] Kharchenko, V., Big Data and Internet of Things for Safety Critical Applications: Challenges, Methodology and Industry Cases, *International Journal on Information Technologies and Security (IJITS)*, 4 (vol. 10), 2018, pp. 6-7.

Information about the author:

Eng. Yoana A. Ivanova – Teaching assistant in the Department of Informatics at NBU; Area of scientific research: Applications of Information Technologies in Security, Communication and Information Systems and Technologies in Security; Professional area: 5.3. "Communication and computer equipment"; Doctoral Program: "Automated Systems for Information processing and Management".

Manuscript received on 10 January 2019
(revised version received on 8 February 2019)