BULGARIAN ACADEMY OF SCIENCES

CYBERNETICS AND INFORMATION TECHNOLOGIES • Volume **22**, No 2
Sofia • 2022 Print ISSN: 1311-9702; Online ISSN: 1314-4081
DOI: 10.2478/cait-2022-0018

Modelling Activity of a Malicious User in Computer Networks

Andon D. Lazarov[1,2], *Petia Petrova*[3]

[1]*Information Technology Department, Nikola Vaptsarov Naval Academy, Varna, Bulgaria*
[2]*Faculty of Aerospace Engineering, K.N. Toosi University of Technology, Tehran, Iran*
[3]*Burgas Free University, Burgas, Bulgaria*
E-mails: a.lazarov@naval-acad.bg ppetrova83@abv.bg

Abstract: *In the present study, an extended classification of Internet users penetrating in computer networks and a definition of the motivation as a psychological and emotional state and main prerequisites for modelling of network intruder's activity are suggested. A mathematical model as a quadratic function of malicious individual's behavior and impact on the computer network based on three quantified factors, motivation, satisfaction and system protection is developed. Numerical simulation experiments of the unauthorized access and its effect onto the computer network are carried out. The obtained results are graphically illustrated and discussed.*

Keywords: *Cybersecurity, Cyberattack, Hacker Psychology, Hacker Behavior Modelling.*

1. Introduction

Network technology allows sharing, delivering and receiving information from any point on the globe. Despite enormous advantages of computer data exchange, the information becomes susceptible to criminal activity, which causes billions of dollars of damage to business, governments and industry. A new term in the computer terminology emerged – hacker. It is a generic term to describe people who are adept at manipulating and attacking computer networks. The scope of the problem caused by the hacker activity can be disclosed analysing computer networks functionality under hackers' attacks and the motivation and behaviour of the unauthorized internet malicious user – the hacker.

Hacker's activity has two basic sides – technological and psychological. The technological characteristics disclose the type and manner of hacking at-tacks to which can be referred [1]:

- Eavesdropping: Using packet sniffers to observe patterns of traffic;
- Snooping: Unauthorized downloading data, an intruder listening to traffic between two machines on the computer network;

- Tampering or data diddling, when the attacker makes an unauthorized modification to data or software on a system;
- Spoofing: the act of disguising a communication from an unknown source as being from a known, trusted source;
- Injecting malicious code: when an attacker exploits an input validation flaw in software to inject malicious code;
- Exploiting flaws in system design, implementation or operation: system vulnerabilities are flaws in a software system's architecture and specification;
- Cracking Passwords, Codes, and Keys known as brute force attacks.

Two or more techniques can be applied in a given hacker attack to achieve the goals of the penetration. For instance, hackers can apply the following sequence of attacks: jamming, spoofing, injection of malicious code. The accent of the present work is on the psychological characteristics that define the motivation of hacker activity and the effect of the unauthorized access to computer information systems. Analysts define hacking as an over interest in computer systems and networks, electronic devices and technological innovations. Intrusion into restricted areas has always been part of testing the ability of a machine and its operators [2, 3]. There are two terms, hackers and crackers to distinguish the behaviour of intruders based on their intentions to act in information territories with restricted access [4, 5]. The first term discloses the concept of gleeful pleasure and satisfaction by elite competition, the second term emphasizes on the criminal essence of the intent for computer network penetration.

The goal of the present work is to analyse the effect of the hacker's influence on computer network and main factors determining the hacker's motivation, to create a mathematical model of hacker's behaviour. The mathematical model describes the dynamics of the hacker's activity, and the evaluation of the hacker's impact in technical, economical and socio-ethical and moral aspects.

In accordance with the defined goal, the rest of the paper is organized in the following sections. In Section 2, the motivation as the psychological and emotional state of the individual is defined. In Section 3, the specific motivations of the user in case of unauthorized access to the network are described. In Section 4, a mathematical model of behaviour and effect of the malicious activity is suggested. In Section 5, the results of modelling of the behaviour and the effect of unauthorized access to the computer network are presented and discussed. In Section 6, conclusion remarks and forecast for future research are made.

2. Motivation as a psychological and emotional state of the individual

Motivation is an inner emotional and psychological state of the individual that causes strength, persistence, and maintains behaviour of the individual to achieve certain goals. Psychologists disclose proportionality and stable relationship between motivation and the result or achievements of the activities. The motivation stimulates the individuals to be active and persistence in performing their intentions [6, 7]. A person without any inspiration to activity can be considered unmotivated, and one who is focused on a specific activity and goal is considered motivated.

There are two types of motivation: intrinsic motivation and extrinsic motivation. What are the factors that rule the behaviour of the intrinsic motivated individual? It could be incentives, values, beliefs, self-esteem, over-ego or just selfishness, momentary or lasting moods and psychological states and more. The intrinsic motivation is related to personality traits and that is why some people have a strong desire to achieve a certain goal or a relentless interest in activities. This stimulate them to work hard and always be active. Intrinsic motivation is the spontaneous attitude to discover and overcome challenges on the way of achieving personal goals, and satisfying particular needs and interests [8, 9].

The extrinsic motivation as a person's temporary state is defined by external circumstances as business, economic, social, political, religion, and more positions, attitudes and relationships.

3. Extended classification of hackers

Hackers' motivations or the motives behind their action are heterogeneous, which allows intruders to be classified into several groups. Unauthorized access is an illegal access or intrusion into computer systems to obstruct the operation or performance of the system or destroy its contents, to the extent corresponding to vandalism. The range of interests and motives that provoke hackers to gain unauthorized access includes attempts to infiltrate secure computer networks without permission, use the Internet to promote terrorism, vandalism, credit card theft, identity theft, intellectual property theft, network distortion or software corruption [10].

In that sense, the intruders with these types of activities that harm society are called black hat hackers, crackers or just criminals. Another type of intruders are white hat hackers, intelligent hackers who help governments or institutions stop crackers from serial attacks and even expose them. They can be called ethical hackers because they have noble intentions.

Computer hackers are regarded as skilled programmers and computer experts who focus on software, computer and network vulnerabilities and are generally categorized as white hats and black hats. There exist terms as grey hats, pen testers, ethical hackers, crackers and hacktivists, script kiddies to distinguish differently motivated hackers.

Today, hackers have a broad spectrum of incentives for their activities. White hats are security analysts and intrusion detection specialists who spend their time just as police or intelligence analysts do – researching the technologies, methodologies, techniques and practices of hackers, in an effort to defend information assets and also detect, prevent and track hackers [11]. White hats do respect applicable laws. In a dichotomy world, they are the good people. Their incentive is to protect software, computers, networks and the IT infrastructures from the bad people, the so-called black hats or crackers.

Grey hats are hackers whose intentions are not fundamentally malicious, but who accept irregular compliance with the law to reach their objectives, which distinguishes them from white hats. Contrary to black hats, greed is not their typical main incentive [12]. Grey hats might also share some incentives with white hats and

so-called true hackers: personal fun, peer recognition, intellectual challenges, etc. However, they do not really share the original hacker ethic.

Ethical hackers act with noble motives that help their organization and colleagues, without expecting material gain. They choose not to use their expertise for malicious purpose. Ethical hackers have their own values and moral principles at personal level, Ethical hackers also have their own values and moral principles on a personal level. However, if their ethical values conflict with those at the public level, their ethical assessment should be reconsidered in the context of the public interest [13].

In the age of information technology, the world depends entirely on the Internet. Disruption of Internet services and other information infrastructure can paralyze a system, an organization, the entire country, and the world at large. This creates a new paradigm and additional incentives for hacking activities.

As a direct consequence, the following categories of hackers have emerged state-sponsored hackers, spy hackers, or even cyber hackers. While white hats provide cybersecurity protect and act against cybercrime, state-sponsored hackers or cyberterrorists have led to new concepts such as cyber warfare, cyber defence and cyber-peace [14-16].

4. Mathematical model of behaviour and effect of a malicious individual's impact

Mathematical modeling of psychological states and human reactions in different activities and circumstances are in the focus of researches in recent years. Risk averseness and emotional stability in e-commerce is discussed in [17, 18]. Specific students' attitudes and reaction to e-learning processes are considered in [19, 20]. Modelling of hacker's unauthorized access to computer networks helps to evaluate and predict future activity (hacking) in order to protect further harms. Based on the statistical theory a discriminant model is developed to categorize an individual's likelihood of engaging in illegal hacking behaviour [21]. The model independent variables include age, gender, education level, professional status, and personal moral philosophy. The model dependent variable is behaviour (measured by willingness to hack), mediated by attitude toward hacking.

An expanded review of hacker behaviour's theoretical statements and principles from point of view of cybersecurity is suggested in [22]. It gives an interdisciplinary description that includes behavioural cybersecurity, human factors, and modelling, and simulation. Hypotheses regarding the hacker's activity and risk of computer hacking detection are considered and tested in [23]. Individuals with low self-control will be more likely to hack, regardless of the likelihood of detection. Youth with intensive use of computers engaged in piracy and spending more time with peers, with weaker parental attention and supervision will be more likely to hack without fear of detection. Males are more likely to hacking behaviour regardless of risk of detection. The above shows the gendered nature of hacking [24]. Analysis of hackers' activity and cybersecurity issues in the maritime industry is discussed in [25].

Many specific factors define the hacker's intrinsic motivation for action, as a specific goal or result of the impact, personal need to act as an expert, social need or the need to conduct a study of information system under attack. The level of satisfaction achieved by hacker's activity is determined by the evaluation of the expected results. This is an integral parameter that includes strength of personal motive and interest, degree of financial benefit, moral and social motive, satisfaction of internal personal needs, etc.

Based on the analysis of the intruders' motivation, three main features should be considered while modelling hackers' behaviour and the state of the information system. First, this is a hacker's level of motivation to achieve a certain goal. Second – the hacker's level of satisfaction. Third is the state of the in-formation system, called level or degree of information system's protection, i.e., level of achieving a satisfactory result from the hacker's impact.

Combining these three factors into one parameter, the effect of the hacker's action *S*, the behaviour of the hacker can be described by a quadratic function and a curve of the second degree with a pronounced maximum at a certain point in time. The result of the hacker's actions is modelled with the following analytical expression:

$$S = \frac{1}{A.\sqrt{1+\left(B.t-\frac{C}{t}\right)^2}}, \quad (1)$$

where *A* is the degree or level of protection in the system, *B* is the degree or level of motivation, *C* is the degree or level of satisfaction with the actions of the hacker, *t* is the current time of the hacker's action. The maximum effect of the hacker's action is defined by equation

$$B.t-\frac{C}{t}=0, \text{ or } B.t=\frac{C}{t}, \quad (2)$$

where the moment of maximum effect of the hacker's impact on the network system of an individual organization or individual user can be determined by expression

$$t_0=\sqrt{\frac{C}{B}}. \quad (3)$$

As follows from the expression (3), with a proportional change in the level of motivation and the level of satisfaction, the parameter t_0 remains unchanged. When the level of satisfaction increases at a relatively constant level of motivation, the parameter t_0 increases. Conversely, when the level of motivation *B* increases at a relatively constant level of satisfaction *C*, the parameter t_0 decreases. As follows from the expression (1), at high values of protection *A*, the maximum effect of the impact of the hacker's penetration decreases.

Based on the observation of hackers' activities in Internet and practical network experience in maintenance of information systems, the values of the system protection, hacker's motivation and satisfaction vary in the interval from 1 to 100.

5. Numerical experimental results of hacker's behaviour and effect of unauthorized penetration

Two numerical simulation experiments have been carried out. In the first experiment, the protection level of the system decreases whereas the *C*/*B* ratio changes with increasing the level of satisfaction results, i.e., the moment of achieving the maximum effect of the hacker's action is different. Fig. 1 presents the effect of the malicious intrusion in the following characteristics of the system and the behaviour of the hacker: level of system's protection $A = 10$, level of motivation $B = 2$, level of achieving a satisfactory result $C = 18$. The moment of the maximal effect is 3, and the result of hacker's action $S = 0.1$.

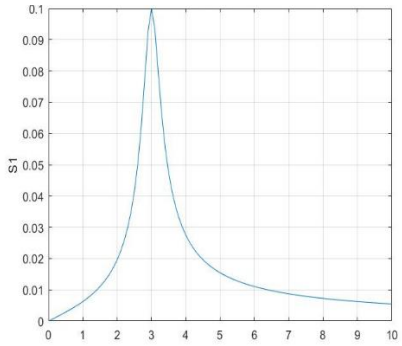

Fig. 1. The effect of the malicious intrusion: $A = 10$, $B = 2$, $C = 18$

Fig. 2 shows the effect of the malicious penetration in the following characteristics of the system and the behaviour of the hacker: level of system's protection $A = 3.8$, level of motivation $B = 2$, level of achieving a satisfactory result $C = 32$. The moment of the maximal effect is 4, and the result of hacker's action $S = 0.27$.

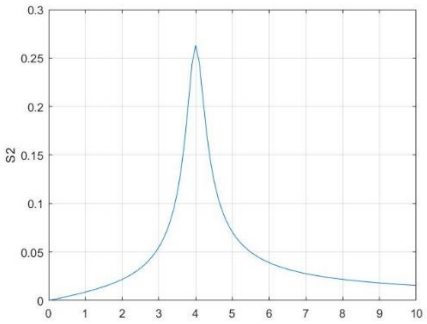

Fig. 2. The effect of the malicious penetration: $A = 3.8$, $B = 2$, $C = 32$

Fig. 3 shows the effect of the malicious intrusion in the following characteristics of the system and the behaviour of the hacker: level of system's protection $A = 1.2$, level of motivation $B = 2$, level of achieving a satisfactory result $C = 50$. The moment of the maximal effect is 5, and the result of hacker's action $S = 0.83$.

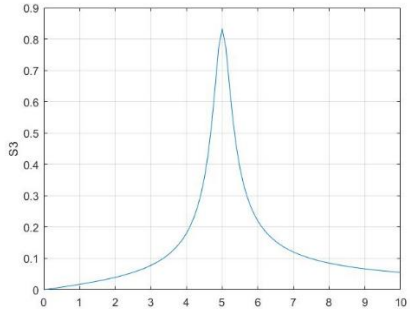

Fig. 3. The effect of the malicious penetration: $A = 1.2$, $B = 2$, $C = 50$

Fig. 4 presents the curves describing the hacker penetration effect in the three scenarios. It follows from the comparison of the curves, that with the decrease in the level of the system's protection and increase the level of satisfaction, the effect of hacker's impact is maximum and displaced in time.

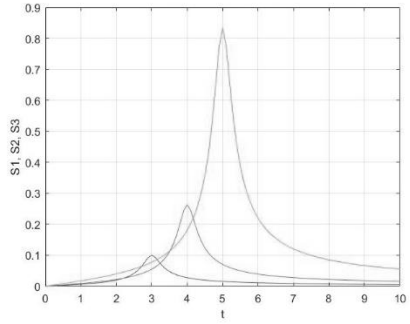

Fig. 4. The effect of the hacker behaviour in the three scenarios

In the second experiment, the C/B ratio remains unchanged with proportional increase of both parameters C and B, i.e., the moment of achieving the maximum effect of the hacker's action is unchanged. This scenario is closer to real behaviour of the hacker, when the motivation and satisfaction proportionally change.

Fig. 5 presents effect of the malicious penetration in the following characteristics of the system and the behaviour of the hacker: level of the system's protection $A = 10$, level of motivation $B = 2$, level of achieving a satisfactory result $C = 18$.

Fig. 6 shows the effect of the malicious intrusion in the following characteristics of the system and the behaviour of the hacker: level of the system's protection $A = 10$, level of motivation $B = 3$, level of achieving a satisfactory result $C = 27$. The moment of the maximal effect is 3, and the result of hacker's action $S = 0.26$.

Fig. 7 shows the impact of malicious penetration in the following characteristics of the system and the behaviour of the hacker: level of the system's protection $A = 10$, level of motivation $B = 4$, level of achieving a satisfactory result $C = 36$. The moment of the maximal effect is 3, and the result of hacker's action $S = 0.84$.

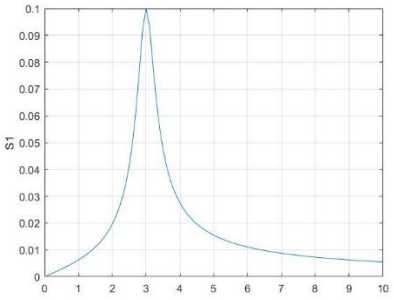

Fig. 5. The effect of the of malicious penetration: $A = 10$, $B = 2$, $C = 18$

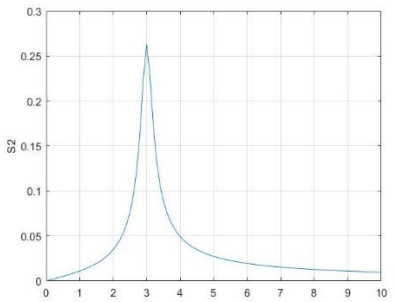

Fig. 6. The effect of the malicious intrusion in the following characteristics of the system and the behaviour of the hacker: $A = 10$, $B = 3$, $C = 27$

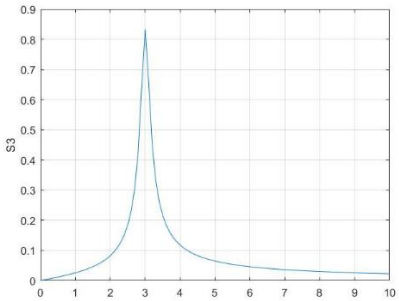

Fig. 7. The effect of the malicious penetration in the following characteristics of the system and the behaviour of the hacker: $A = 10$, $B = 4$, $C = 36$

Fig. 8 presents the curves of the impact effect in the three scenarios. From the comparison of the curves, it follows that in case of constant level of the system's protection and proportional change of the motivation and satisfaction, the effect of the hacker's impact increases at the moment of functional extremum.

It means that in these circumstances, constant level of the system protection and proportionality of the motivation and satisfaction, the effect of hacker's activity does not depend of a system protection and depends only on psychological individual's factors as motivation and satisfaction of results achieved.

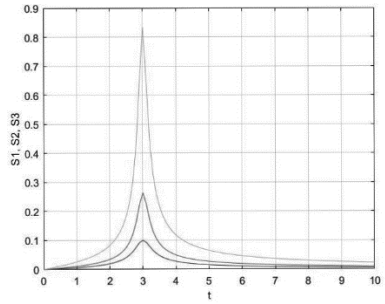

Fig. 8. The effect of the hacker behaviour in the three scenarios

6. Conclusion

An extended hackers' classification, and an analysis of the behaviour as well as the effect of the unauthorized malicious user (hacker) activity on a computer system are suggested in the present work. The mathematical model of the malicious individual's behaviour is created based on observations and measurements of hackers' activity in the communication and information space. An analytical expression describes the dynamics of the unauthorized user's behaviour and the state of the information system in time. Three key factors determine the shape of the hacker behaviour's curve: motivation and satisfaction of the activity, and the state of the information system.

As a future trend the derived mathematical formula, modelling the behaviour of a malicious user with unauthorized access rights, can be used to model intruders' behaviour and extrapolate their actions in the computer network. The value of the invariant parameters of the model can be determined for each specific case of malicious activity and specific role of the local network. Observations of a particular hacker's behaviour allow building his/her specific signature and recording in hacker activity's data base. This allows, activities of hackers to be easy recognized in order to take appropriate counter measures.

References

1. Z a k a r a s, M. R. International Computer Crimes. – General Report, Vol. **72**, 2001, No 3-4, pp. 813-829. Last access 200021/11/14.
   https://www.cairn.info/revue-internationale-de-droit-penal-2001-3-page-813.htm
2. B r d i c z k a, O., J. L i u, B. P r i c e, J. S h e n. Proactive Insider Threat Detection Through Graph Learning & Psychological Context. Palo Alto Research Centre.
   http://www.ieee- se-curity.org/TC/SPW2012/proceedings/4740a142.pdf
3. Anonymous. The Difference Between Hackers and Crackers. Maximum Security, Indiana: Pearson/ Que, 2002.
   http://www.informit.com/articles/article.aspx?p=30048
4. J e l e n, S. Hacker vs. Cracker. TechRepublic, 14 Oct 2021.
   https://securitytrails.com/blog/hacker-vs-cracker
5. P a s s e r i, P. Cyber Attack Statistics. Hackmageddon.com, 2014.
   http://hackmageddon.com/
6. C h a n, S. H. An Empirical Investigation of Hacking Behaviour. – The Review of Business Information Systems, Vol. **9**, 2005, No 4, pp. 42-52.

7. W e i n s t e i n, B. Should You Hire an Ex-Hacker. TechRepublic, 11 June 2002, **https://www.techrepublic.com/article/should-you-hire-an-ex-hacker/.**
8. C h a n, S. H., L. J. Y a o. An Exploratory Study on Systems Security and Hacker Hiring. – The Review of Business Information Systems, Vol. **8**, 2004, pp. 17-28.
9. L a w a t i, E. A., S. B a s h a, G. B h a t t a c h a r y a, J. H a s h m i. Mathematical Model and Unitization for the Behaviour of the Intrinsic Recreation Hackers. – International Journal of Innovative Research in Advanced Engineering (IJIRAE), Vol. **1**, (2014), No 8. ISSN: 2349-2163.
10. B a r b e r, R. Hackers Profiled – Who Are They and What Are Their Motivations? – Computer Fraud Secur, Vol. **2**, 2001, pp. 14-17.
11. O l s o n, P. We are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency. New York, Back Bay Books, 2013.
12. B r a t u s, S. What Hackers Learn That the Rest of Us Don't Notes on Hacker Curriculum? – IEEE Secur. Priv, Vol. **5**, 2007, No 4, pp. 72-75.
13. J a q u e t-C h i f f e l l e, D. O., M. L o i. Ethical and Unethical Hacking, Part of the International Library of Ethics. – Law and Technology Book Series (ELTE), Vol. **21**, 2020. **https://link.springer.com/chapter/10.1007/978-3-030-29053-5_9**
14. Australian Government, Australian Institute of Criminology, Australian High-Tech Crime Centre, 2005. **https://www.aic.gov.au/sites/default/files/2020-05/htcb005.pdf.**
15. M a r s h a l l, A. K. Digital Forensics: Digital Evidence in Criminal Investigations. London, Wiley-Blackwell, 2008. **https://www.wiley.com/en-us/Digital+Forensics%3A+Digital+Evidence+in+Criminal+Investigations-p-9780470517741**
16. M o h u r l e, S., P a t i l, M. A Brief Study of Wannacry Threat: Ransomware Attack. – International Journal Advance Research Computer Science, Udaipur, Vol. **8**, 2017, No 5. **https://search.proquest.com/docview/1912631307/abstract/DEF9AE2FF2924E35PQ/**
17. P o p c h e v, I., R. K e t i p o v, V. A n g e l o v a. Risk Averseness and Emotional Stability in e-Comers. – Cybernetics and Information Technologies, Vol. **21**, 2021, No 3, pp. 74-84.
18. P o p c h e v, I., I. R a d e v a. A Decision Support Method for Investment Preference Evaluation. – Cybernetics and Information Technologies, Vol. **6**, 2006, No 1, pp. 3-16.
19. P o p c h e v, I., D. O r o z o v a. Towards a Multistep Method for Assessment in e-Learning for Emerging Technologies. – Cybernetics and Information Technologies, Vol. **20**, 2020, No 3, pp. 116-129.
20. P o p c h e v, I., D. O r o z o v a. Towards Big Data Analytics in the e-Learning Space. – Cybernetics and Information Technologies, Vol. **19**, 2019, No 3, pp. 16-24.
21. B e e b e, N., J. C l a r k. A Model for Predicting Hacker Behaviour. – Published in AMCIS 1, Psychology, Computer Science, 2006.
22. L a h c e n, M., R. A. C a u l k i n s, B. M o h a p a t r a et al. Review and Insight on the Behavioural Aspects of Cybersecurity. – Cybersecurity, Vol. **3**, 2020, No 10. **https://doi.org/10.1186/s42400-020-00050-w**
23. L e e, J. R., T. J. H o l t. Assessing the Factors Associated with the Detection of Juvenile Hacking Behaviours. – Front. Psychol, 5 May 2020. **https://doi.org/10.3389/fpsyg.2020.00840**
24. D o h r e n, J. Inside the Mind of a Hacker. 2021. **https://www.pwc.ch/en/insights/digital/inside-the-mind-of-a-hacker.html**
25. M e d n i k a r o v, B., Y. T s o n e v, A. L a z a r o v. Analysis of Cybersecurity Issues in the Maritime Industry. – Information & Security: An International Journal, Vol. **47**, 2020, No 1, pp. 27-43. ISSN 0861-5160. **https://doi.org/10.11610/isij.4702**

Received:17.11.2021; Second Version: 21.03.2022; Accepted: 31.03.2022