DOCUMENT

Name and surname	doc. RNDr. PaedDr. Ladislav Huraj, PhD.
Document type:	Characteristics of the submitted research/ artistic/other output
The name of the university	University of Ss. Cyril and Methodius in Trnava
The seat of the university	Nám. J. Herdu 2, 917 01 Trnava
The name of the faculty	Faculty of Natural Sciences
The seat of the faculty	Nám. J. Herdu 2, 917 01 Trnava

Surname awarded to the assessed person

Huraj

Name awarded to the assessed person

Ladislav

Degrees awarded to the assessed person

doc. RNDr. PaedDr., PhD.

Hyperlink to the entry of the person in the Register of university staff

https://www.portalvs.sk/regzam/detail/14469

Area of assessment

Applied informatics

Category of the research/ artistic/other output

scientific output

Year of publication of the research/artistic/other output

2020

ID of the record in the Central Registry of Publication Activity (CRPA) or the Central Registry of Artistic Activity (CRAA)

ID = 212906

Hyperlink to the record in CRPA or CRAA

https://app.crepc.sk/?fn=detailBiblioFormChildM1L315&sid=393B45DF84C5274BD01FD974B9&seo=CREP%C4%8C-detail-%C4%8Cl%C3%A1nok

Hyperlink to the record in another publicly accessible register, catalogue of research/ artistic/other outputs

https://www.webofscience.com/wos/woscc/full-record/WOS:000581974200001

Hyperlink to the webpage where the output is available (full text, other documentation, etc.)

https://www.mdpi.com/1424-8220/20/18/5298

Characteristics of the author's contribution

As stated in the article itself in the "Author Contributions" section, the main author's contribution of the evaluated person (40%) consists of the following parts when solving the problem: concept, methodology, validation, the research itself, writing - original preparation of the concept, and funding acquisition. In addition, one of the co-authors of the article was a doctoral student of the evaluated person at the time of publication of the output.

Annotation of the output with contextual information concerning the description of creative process and the content of the research/artistic/other activity, etc.

Huraj, L.; Šimon, M.; Horák, T. Resistance of IoT Sensors against DDoS Attack in Smart Home Environment. Sensors 2020, 20, 5298. (CC, WoS, IF 3.275)

Annotation of the output in English

Smart devices along with sensors are gaining in popularity with the promise of making life easier for the owner. As the number of sensors in an Internet of Things (IoT) system grows, a question arises as to whether the transmission between the sensors and the IoT devices is reliable and whether the user receives alerts correctly and in a timely manner. Increased deployment of IoT devices with sensors increases possible safety risks. It is IoT devices that are often misused to create Distributed Denial of Service (DDoS) attacks, which is due to the weak security of IoT devices against misuse. The article looks at the issue from the opposite point of view, when the target of a DDoS attack are IoT devices in a smart home environment. The article examines how IoT devices and the entire smart home will behave if they become victims of a DDoS attack aimed at the smart home from the outside. The question of security was asked in terms of whether a legitimate user can continue to control and receive information from IoT sensors, which is available during normal operation of the smart home. The case study was done both from the point of view of the attack on the central units managing the IoT sensors directly, as well as on the smart-home personal assistant systems, with which the user can control the IoT sensors. The article presents experimental results for individual attacks performed in the case study and demonstrates the resistance of real IoT sensors against DDoS attack. The main novelty of the article is that the implementation of a personal assistant into the smart home environment increases the resistance of the user's communication with the sensors. This study is a pilot testing the selected sensor sample to show behavior of smart home under DDoS attack.

List of maximum 5 most significant citations corresponding to the output

1. Onesimu, J.A., Karthikeyan, J. & Sei, Y. An efficient clustering-based anonymization scheme for privacy-preserving data collection in IoT based
healthcare services. Peer-to-Peer Netw. Appl. (2021). https://doi.org/10.1007/s12083-021-01077-7 (Scopus, WoS)
2. Ma, Xiaohao, Zhengfan Jiang, and Yuanjing Lin. Flexible energy storage devices for wearable bioelectronics. Journal of Semiconductors 42 (2021): 1-12. (Scopus,WoS)
3. Mishra N, Pandya S, Patel C, Cholli N, Modi K, Shah P, Chopade M, Patel S, Kotecha K. Memcached: An Experimental Study of DDoS Attacks for the Wellbeing of IoT Applications. Sensors. 2021; 21(23):8071. https://doi.org/10.3390/s21238071 (Scopus, WoS)
4. Ibraheem N.A., Abdulhadi N.M., Hasan M.M. (2022) Merging Data Analytics and Machine Learning Algorithm for Home System Security-Based Internet of Things. In: Ranganathan G., Fernando X., Shi F., El Allioui Y. (eds) Soft Computing for Security Applications. Advances in Intelligent Systems and Computing, vol 1397. Springer, Singapore. https://doi.org/10.1007/978-981-16-5301-8_35 (Scopus)
5. Zhao, J., Xiang, M. M., Song, X., Tian, C., & Yang, Y. (2020). The Application and Threat of the Internet of Things in the Smart Grid. In 2020 2nd International Conference on Applied Machine Learning (ICAML) (pp. 339-343). IEEE. (Scopus)

Characteristics of the output's impact on socio-economic practice

The article describes a case study of a DDoS attack on IoT devices in a smart home environment and the impact of the attack on communication and control of IoT sensors from the perspective of a user using smart home services. In general, it can be concluded that the experimental results showed that an external DDoS attack on IoT devices in a smart home environment can be successful and have a significant impact on the communication and control of IoT sensors inside the smart home environment. The method of communicating with user IoT sensors through a personal smart-home assistant application has proven to be the safest way to control an IoT sensor. The integration of the system of personal smarthome assistants into the smart home environment not only solves the problem of technological fragmentation that arises during the implementation of the smart home ecosystem, but also increases the resistance of user communication with IoT sensors to DDoS attacks conducted from the external environment. This fact is the main contribution of the article.

Characteristics of the output and related activities' impact on the educational process

The problem solved in the output (cyber attacks and defense against them) has a direct impact on the subject Information Security , which is taught by the assessed person. The problem solved in the output directly corresponds to the contents of this subject, both methodologically (used methods of attack and defense), but also technically (used software and hardware) and will positively influence the educational process. The impacts can also be seen indirectly in the Project Management subject.
In addition, the security of IoT devices is the topic of a number of final theses that the evaluated person leads in the study program. The article is also followed by foreign final theses, e.g. : Isah, R.E. (2022). The vulnerability studies and security postures of smart home devices (Master's thesis, Altınbaş Üniversitesi, Turkey). Agarwal, R. (2021). Graph-Based Simulation for Cyber-Physical Attacks on Smart Buildings (Doctoral dissertation, Virginia Tech, USA).

Area of assessment

Applied informatics

Category of the research/ artistic/other output

scientific output

Year of publication of the research/artistic/other output

2018

ID of the record in the Central Registry of Publication Activity (CRPA) or the Central Registry of Artistic Activity (CRAA)

ID = 88263

Hyperlink to the record in CRPA or CRAA

https://app.crepc.sk/?fn=detailBiblioFormChildK1LDKI&sid=D1CFA2C0538D9116B40F08E4&seo=CREP%C4%8C-detail-kapitola-/-pr%C3%Adspevok

Hyperlink to the record in another publicly accessible register, catalogue of research/ artistic/other outputs

https://www.webofscience.com/wos/woscc/full-record/WOS:000465218500036

Hyperlink to the webpage where the output is available (full text, other documentation, etc.)

https://ieeexplore.ieee.org/document/8524703

Characteristics of the author's contribution

The evaluated person participated as the main author (50%) in all phases of the creation of the output, from the design of the solution concept, through experimental testing, analysis of the achieved results, to the process of writing the article and incorporating review recommendations. In addition, one of the coauthors of the article was a doctoral student of the evaluated person at the time of publication of the output.

Annotation of the output with contextual information concerning the description of creative process and the content of the research/artistic/other activity, etc.

Huraj, L., Šimon, M., and Horák, T.: IoT Measuring of UDP-Based Distributed Reflective DoS Attack. In: IEEE 16th International Symposium on Intelligent Systems and Informatics (SISY 2018). IEEE, Serbia, 2018, pp. 209-214.

Annotation of the output in English

IoT devices and their fast growth on the Internet cause many cyber-attacks problems. The number of compromised IoT devices can be used by DDoS (Distributed Denial of Service) attackers to imitate valid request packet or to form illegal request packet to the victim with a spoofed source IP addresses to hide themselves, meanwhile giving rise the system collapse, the obstruction of network/traffic, or disrupting of the victim Internet operation. In this article is demonstrated a specific kind of DDoS attack involving usually accessible IoT devices -the UDP-based Distributed Reflective DoS Attack (DRDoS). The packets are flooded by the attacker to the IoT device as a reflector with a source IP address set to the IP address of the victim who obtains the reflected replies and can be overloaded. To examine this kind of attack, there has to be four representatives of heterogeneous IoT devices involved: an IP camera, a smart light-bulb, a network printer, and a small single-board computer Raspberry Pi. This article illustrates the possibility of the IoT devices to be integrated into DRDoS attack and to flood a network as well as their potential to form a targeted attack on a particular victim machine.

List of maximum 5 most significant citations corresponding to the output

1. Aljuhani, A. (2021). Machine Learning Approaches for Combating Distributed Denial of Service Attacks in Modern Networking Environments. IEEE Access , 9, 42236-42264. (Scopus, WoS)
2. Gondim, João JC, Robson de Oliveira Albuquerque, and Ana Lucila Sandoval Orozco. "Mirror saturation in amplified reflection Distributed Denial of Service: A case of study using SNMP, SSDP, NTP and DNS protocols." Future Generation Computer Systems (2020). (WoS,Scopus)
3. Samaila, M. G., Sequeiros, J. B., Simões, T., Freire, M. M., & Inácio, P. R. (2020). IoT-HarPSecA: A Framework and Roadmap for Secure Design and Development of Devices and Applications in the IoT Space. IEEE Access . (Scopus,WoS)
4. Waraga, O. A., Bettayeb, M., Nasir, Q., & Talib, M. A. (2020). Design and implementation of automated IoT security testbed. Computers & Security, 88, 101648. (Scopus, WoS)
5. Bettayeb, M., Waraga, O. A., Talib, M. A., Nasir, Q., & Einea, O. (2019, November). IoT Testbed Security: Smart Socket and Smart Thermostat. In 2019 IEEE Conference on Application, Information and Network Security (AINS) (pp. 18-23). IEEE. (WoS,Scopus)

Characteristics of the output's impact on socio-economic practice

The article belongs to a series of research tasks solved within the VEGA and APVV project focused on network security. The output demonstrates the vulnerability of a selected group of IoT devices against DDoS attacks. Among other things, the article points to the original finding that it is generally not possible to use IoT devices to create a targeted reflected DDoS attack on a specific victim computer; but this kind of attack makes sense in specific situations where the attack is aimed at a large number of IP addresses routing over a normal network connection in a way to overwhelm the connection. Although this is a conference paper, the output has since been cited in a wide variety of IoT device security areas, e.g. DDoS attacks on IoT devices, building IoT test environments, or reflected DDoS attacks in 5G networks.

Characteristics of the output and related activities' impact on the educational process

The problem solved in the output (cyber attacks and defense against them) has a direct impact on the subject Information Security , which is taught by the assessed person. The problem solved in the output directly corresponds to the contents of this subject, both methodologically (used methods of attack and defense), but also technically (used software and hardware) and will positively influence the educational process. The impacts can also be seen indirectly in the Project Management subject. In addition, the security of IoT devices is the topic of a number of final theses that the evaluated person leads in the study program.

Area of assessment

Applied informatics

Category of the research/ artistic/other output

scientific output

Year of publication of the research/artistic/other output

2021

ID of the record in the Central Registry of Publication Activity (CRPA) or the Central Registry of Artistic Activity (CRAA)

ID = 250414

Hyperlink to the record in CRPA or CRAA

https://app.crepc.sk/?fn=detailBiblioFormChildK1DHHU&sid=D16FD961663FDD94FFEB63029A&seo=CREP%C4%8C-detail-%C4%8Cl%C3%A1nok

Hyperlink to the record in another publicly accessible register, catalogue of research/artistic/other outputs

https://www.webofscience.com/wos/woscc/full-record/WOS:000632078900001

Hyperlink to the webpage where the output is available (full text, other documentation, etc.)

https://www.mdpi.com/2076-3417/11/4/1847

Characteristics of the author's contribution

As stated in the article itself in the "Author Contributions" section, the main author's contribution of the evaluated person (40%) consists of the following parts when solving the problem: concept, methodology, formal analysis, research itself, sources, writing - original preparation of the concept, writing - review and editing, supervision and funding acquisition. In addition, one of the co-authors of the article was a doctoral student of the evaluated person at the time of publication of the output.

Annotation of the output with contextual information concerning the description of creative process and the content of the research/artistic/other activity, etc.

Huraj, L.; Horak, T.; Strelec, P.; Tanuska, P. Mitigation against DDoS Attacks on an IoT-Based Production Line Using Machine Learning. Appl. Sci. 2021, 11, 1847. https://doi.org/10.3390/app11041847 (CC, WoS, IF 2.679, Q2)

Annotation of the output in English

Industry 4.0 collects, exchanges, and analyzes data during the production process to increase production efficiency. Internet of Things (IoT) devices are among the basic technologies used for this purpose. However, the integration of IoT technology into the industrial environment faces new security challenges that need to be addressed. This is also true for a production line. The production line is a basic element of industrial production and integrating IoT equipment allows one to streamline the production process and thus reduce costs. On the other hand, IoT integration opens the way for network cyberattacks. One possible cyberattack is the increasingly widely used distributed denial-of-service attack. This article presents a case study that demonstrates the devastating effects of a DDOS attack on a real IoT-based production line and the entire production process. The emphasis was mainly on the integration of IoT devices, which could potentially be misused to run DDoS. Next, the verification of the proposed solution is described, which proves that it is possible to use the sampled flow (sFlow) stream to detect and protect against DDoS attacks on the running production line during the production process.

List of maximum 5 most significant citations corresponding to the output

1. Zachos, Georgios, et al. "An Anomaly-Based Intrusion Detection System for Internet of Medical Things Networks." Electronics 10.21 (2021): 2562. (WoS,Scopus).
2. Wijaya, C., Wiryasaputra, R., Wang, I. J., Wu, R. C., & Yang, C. T. (2024). Simulation of DOS Attacks Mitigation in Software Defined Network Architecture using Load Balancing Algorithm. Mobile Networks and Applications, 29(3), 961-980..(WoS,Scopus).
3. Jan, Z., Ahamed, F., Mayer, W., Patel, N., Grossmann, G., Stumptner, M., & Kuusk, A. (2023). Artificial intelligence for industry 4.0: Systematic review of applications, challenges, and opportunities. Expert Systems with Applications, 216, 119456. (WoS,Scopus).
4. Zhao, R., Zuo, Z., Wang, Y., & Zhang, W. (2023). Active control strategy for switched systems against asynchronous DoS attacks. Automatica, 148, 110765.(WoS,Scopus).
5. Adil, M., Khan, M. K., Kumar, N., Attique, M., Farouk, A., Guizani, M., & Jin, Z. (2024). Healthcare internet of things: Security threats, challenges and future research directions. IEEE Internet of Things Journal.(WoS,Scopus).

Characteristics of the output's impact on socio-economic practice

The article presents a case study that demonstrates the devastating effects of a DDOS attack on a real IoT-based production line and on the entire manufacturing process. DDoS attacks on the infrastructure of the production line are only assumed in the literature, but not empirically confirmed or otherwise documented. A study carried out on a real production line proves the vulnerability of the infrastructure to cyber attacks. In addition, the article demonstrates the effectiveness of the designed defense solution based on sample flow (sFlow) with minimal impact on the running production line during the production process.The article also makes available a test dataset, which is unique from the point of view of cyber DDoS attacks conducted on the production line.

Characteristics of the output and related activities' impact on the educational process

The problem solved in the output (cyber attacks and defense against them) has a direct impact on the subject Information Security, which is taught by the assessed person. The problem solved in the output directly corresponds to the contents of this subject, both methodologically (used methods of attack and defense), but also technically (used software and hardware) and will positively influence the educational process. The impacts can also be seen indirectly in the Project Management subject.
The output is followed by, for example, a Springer publication with a bachelor's student in applied informatics focused on testing DDoS attacks "Comparison of software simulation and network testbed of DDoS attacks for IPv4 and IPv6 networks".

Area of assessment

Applied informatics

Category of the research/ artistic/other output

scientific output

Year of publication of the research/artistic/other output

2013

ID of the record in the Central Registry of Publication Activity (CRPA) or the Central Registry of Artistic Activity (CRAA)

ID = UCM.Trnava.PC014531

Hyperlink to the record in CRPA or CRAA

http://www.crepc.sk/portal?fn=*recview&uid=1076800&pageId=basket&full=0

Hyperlink to the record in another publicly accessible register, catalogue of research/ artistic/other outputs

https://www.scopus.com/record/display.uri?eid=2-s2.0-84881249916&origin=resultslist&featureToggles=FEATURE_NEW_METRICS_SECTI ON:1

Hyperlink to the webpage where the output is available (full text, other documentation, etc.)

https://d1wqtxts1xzle7.cloudfront.net/39962038/Towards_a_VO_Intersection_Trust_Model_fo20151113-30010-1f1fnza-with-cover-pagev2.pdf?Expires=1646170652&Signature=SytGz2WmeLHGH92HfVTexUIZD~7XjXN40rFBak4fGnA0ojRG470v~XCV2pgvGMzsCTvj30O60JvtcniwVnTYMDWckuGZ6L0J3K0QnUb79y4XuV9PTev6zfJzikQi9NbiE~fp1r5ZWSe0GJDJZ9kCn9gE3pIdXM0DuACDdvAAYLtzgqOde2Y6SbFf6MrbB~bGv3f3goe-erq0ZyMAP38x3rnpXWUASPQ~CZ4khJRKqCDUDuq5OKJhMGjo5MHjnPDrRIXo8IPKYpnvVbm~nU1itOer4J1rlPoQVqV7eW0CuWAW~Js5GULR5MNbcLt9BvHkK8Y1ET8j1xMno3fTgabQ__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA

Characteristics of the author's contribution

The evaluated person participated as the main author (50%) in all phases of the creation of the output, from the design of the solution concept, through experimental testing, analysis of the achieved results, to the process of writing the article and incorporating review recommendations.

Annotation of the output with contextual information concerning the description of creative process and the content of the research/artistic/other activity, etc.

Huraj, L., Siládi, V., Škrinarová, J., Bojdová, V.: Towards a VO Intersection Trust Model for Ad hoc Grid Environment: Design and Simulation Results, In: IAENG International Journal of Computer Science, 40:2, May 2013, pp. 53-61, ISSN 1210-0552

Annotation of the output in English

An ad hoc grid environment is a spontaneous organization of cooperating heterogeneous nodes in a logical community without a fixed infrastructure and with only minimal administrative requirements. Trust is an integral part of ad hoc grid computing systems as well. It is not possible to utilize trust principles of traditional grid environment uses various, mostly centrally oriented methods for trust establishment, e.g. certification authorities, VO management servers or credentials pools. An ad hoc grid environment demands minimal administrative requirements; especially an absence of a central trust authority, where collaborating entities must establish and maintain a trust relationship among themselves. Our article presents a design of two algorithms for a supported authorization mechanism in order to more easily form virtual organizations based on attribute certificates. Moreover, an evaluation of the two algorithms, primary and extended algorithm, based on simulation results as well as deeper insights into the configuration of such schemes in ad hoc grid environment are described.

List of maximum 5 most significant citations corresponding to the output

1. Daxing Wang, Jikai Teng: Efficient Aggregate Signature Algorithm and Its Application in MANET, In: International Journal of Mathematical, Computational Science and Engineering Vol:7 No:11, 2013.

Characteristics of the output's impact on socio-economic practice

The output belongs to the field of information security. The article proposes a new authorization mechanism based on the principle of trust for ad hoc grids in such a way that it is possible to more easily create virtual organizations based on attribute certificates. The output is the journal culmination of a series of conference articles by the evaluated person on the issue of trust in ad hoc grids. The output significantly expands previous works in terms of detailed formulation as well as validation of the proposed security solution. Although the largest number of citations to the proposed solutions are to the conference articles of the evaluated person listed in article [3,9,20], which the evaluated person follows up with the output, the output itself is also referred to in an article from the areas of MANET networks.

Characteristics of the output and related activities' impact on the educational process

The problem solved in the output (cyber attacks and defense against them) has a direct impact on the subject Information Security, which is taught by the assessed person. The problem solved in the output directly corresponds to the contents of this subject, both methodologically (used methods of attack and defense), but also technically (used software and hardware) and will positively influence the educational process. The impacts can also be seen indirectly in the Project Management subject.In addition, the security of IoT devices is the topic of a number of final theses that the evaluated person leads in the study program.

Area of assessment

Applied informatics

Category of the research/ artistic/other output

scientific output

Year of publication of the research/artistic/other output

2010

ID of the record in the Central Registry of Publication Activity (CRPA) or the Central Registry of Artistic Activity (CRAA)

ID = UMB.B.Bystrica.0102589

Hyperlink to the record in CRPA or CRAA

http://www.crepc.sk/portal?fn=*recview&uid=146371&pageId=basket&full=0

Hyperlink to the record in another publicly accessible register, catalogue of research/ artistic/other outputs

https://www.scopus.com/record/display.uri?eid=2-s2.0-79958746586&origin=resultslist&featureToggles=FEATURE_NEW_METRICS_SECTI ON:1

Hyperlink to the webpage where the output is available (full text, other documentation, etc.)

http://www.wseas.us/elibrary/ conferences/2010/Corfu/COMPUTERS/COMPUTERS2-44.pdf

Characteristics of the author's contribution

The evaluated person was involved as main author (50%) in all phases of the development of the output, from the of the output, from the actual design of the solution concept, through the experimental testing and analysis of the the analysis of the results obtained, to the process of writing the paper and incorporating review recommendations.

Annotation of the output with contextual information concerning the description of creative process and the content of the research/artistic/other activity, etc.

Huraj, L., Siládi, V, Siláči, J.: Design and Performance Evaluation of Snow Cover Computing on GPUs. In: Proceedings of the 14th WSEAS International Conference on Computers: Latest Trends on Computers, Corfu Island, Greece, July 2010, pp. 674-677, ISBN: 978-960-474-213-4.

Annotation of the output in English

An ad hoc grid environment is a spontaneous organization of cooperating heterogeneous nodes in a logical community without a fixed infrastructure and with only minimal administrative requirements. Trust is an integral part of ad hoc grid computing systems as well. It is not possible to utilize trust principles of raditional grid environment uses various, mostly centrally oriented methods for trust establishment, e.g. certification authorities, VO management servers or credentials pools. An ad hoc grid environment demands minimal administrative requirements; especially an absence of a central trust authority, where collaborating entities must establish and maintain a trust relationship among themselves. Our article presents a design of two algorithms for a supported authorization mechanism in order to more easily form virtual organizations based on attribute certificates. Moreover, an evaluation of the two algorithms, primary and extended algorithm, based on simulation results as well as deeper insights into the configuration of such schemes in ad hoc grid environment are described.

List of maximum 5 most significant citations corresponding to the output

1. Montella, Raffaele, et al. "Workflow-based automatic processing for Internet of Floating Things crowdsourced data." Future Generation Computer Systems , Volume 94, May 2019, Pages 103-119. (WoS,Scopus)
2. Montella, Raffaele, et al. "Marine bathymetry processing through GPGPU virtualization in high performance cloud computing." Concurrency and
Computation: Practice and Experience , 30(24) Article Number: e4895, 2018. (WoS, Scopus)
3. Marcellino, L., et al. "Using GPGPU accelerated interpolation algorithms for marine bathymetry processing with on-premises and cloud based computational resources." Lecture Notes in Computer Science, Volume 10778 LNCS, 2018, Pages 14-24. (WoS, Scopus)
4. Mei, G., Xu, L., & Xu, N. (2017). Accelerating adaptive inverse distance weighting interpolation algorithm on a graphics processing unit. Royal Society Open Science , 4(9), 170436. (WoS, Scopus)
5. Eränen, D., Oksanen, J., Westerholm, J., & Sarjakoski, T. (2014). A full graphics processing unit implementation of uncertainty-aware drainage basin delineation. Computers & Geosciences , 73, pp. 48-60. (WoS, Scopus)

Characteristics of the output's impact on socio-economic practice

The output demonstrates the capabilities of the CUDA architecture, which utilizes the powerful parallel computing capacity of GPUs to accelerate the computational process of snow cover height estimation using the Inverse Distance Weighted (IDW) method. The authors solve the problem of snow cover estimation in cooperation with the Slovak Hydrometeorological Institute. The given output was followed by several other conference and magazine articles of the evaluated person on the given issue aimed at finding a suitable tool for the mentioned issue. Although this is a conference paper, the output has since been cited in a wide variety of areas of interpolation methods and GPGPU use.

Characteristics of the output and related activities' impact on the educational process

The problem solved in the output (task parallelization, parallel processes, programming) has an indirect impact on the subject Theoretical foundations of computer science , which is taught by the evaluated person; primarily in the second part of the subject dedicated to Computational Complexity , where classes of computational complexity and possible solutions to computationally demanding tasks are covered. In addition, the task parallelization is the topic of several of final theses that the evaluated person leads in the study program.