DOKUMENT

Meno a priezvisko	doc. RNDr. PaedDr. Ladislav Huraj, PhD.
Typ dokumentu	Charakteristika predkladaného výstupu tvorivej činnosti
Názov vysokej školy	Univerzita sv. Cyrila a Metoda v Trnave
Sídlo vysokej školy	Nám. J. Herdu 2, 917 01 Trnava
Názov fakulty	Fakulta prírodných vied
Sídlo fakulty	Nám. J. Herdu 2, 917 01 Trnava

OCA1. - Priezvisko hodnotenej osoby

Huraj

OCA2. - Meno hodnotenej osoby

Ladislav

OCA3. - Tituly hodnotenej osoby

doc. RNDr. PaedDr., PhD.

OCA4. - Hyperlink na záznam osoby v Registri zamestnancov vysokých škôl

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

1. hodnotený výstup

OCA5. - Oblasť posudzovania

Aplikovaná informatika

OCA6. - Kategória výstupu tvorivej činnosti

vedecký výstup

OCA7. - Rok vydania výstupu tvorivej činnosti

2020

Charakteristika výstupu, ktorý je registrovaný v CREPČ alebo CREUČ

OCA8. - ID záznamu v CREPČ alebo CREUČ (ak je)

ID = 212906

OCA9. - Hyperlink na záznam v CREPČ alebo CREUČ

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

Charakteristika výstupu, ktorý nie je registrovaný v CREPČ alebo CREUČ

OCA10. - Hyperlink na záznam v inom verejne prístupnom registri, katalógu výstupov tvorivých činností

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

OCA13. - Hyperlink na stránku, na ktorej je výstup sprístupnený (úplný text, iná dokumentácia a podobne)

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

OCA14. - Charakteristika autorského vkladu

Ako je uvedené aj v samotnom článku v časti „Author Contributions“, nosný autorský vklad hodnotenej osoby (40%) pozostáva pri riešení problému z častí: koncept, metodológia, validácia, samotný výskum, písanie - pôvodná príprava konceptu, a získavanie finančných prostriedkov. Navyše jeden zo spoluautorov článku bol doktorandom hodnotenej osoby v čase publikovania výstupu.

OCA15. - Anotácia výstupu s kontextovými informáciami týkajúcimi sa opisu tvorivého procesu a obsahu tvorivej činnosti a pod.

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)

OCA16. - Anotácia výstupu v anglickom jazyku

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.

OCA17. - Zoznam najviac 5 najvýznamnejších ohlasov na výstup

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)

OCA18. - Charakteristika dopadu výstupu na spoločensko-hospodársku prax

Článok popisuje prípadovú štúdiu DDoS útoku na IoT zariadenia v prostredí inteligentnej domácnosti a dopad útoku na komunikáciu a ovládanie IoT senzorov z pohľadu používateľa využívajúceho služby inteligentnej domácnosti. Vo všeobecnosti možno konštatovať, že experimentálne výsledky ukázali, že DDoS útok vedený zvonku na IoT zariadenia v prostredí inteligentnej domácnosti môže byť úspešný a mať významný vplyv na komunikáciu a ovládanie IoT senzorov vo vnútri prostredia inteligentnej domácnosti. Spôsob komunikácie s používateľskými IoT senzormi prostredníctvom aplikácie osobného smart-home asistenta sa ukázal ako najbezpečnejší spôsob ovládania IoT senzoru. Integrácia systému osobných smart-home asistentov do prostredia inteligentnej domácnosti nielenže rieši problém technologickej fragmentácie, ktorá vzniká pri implementácii ekosystému inteligentných domácností, ale tiež zvyšuje odolnosť komunikácie používateľov so senzormi internetu vecí voči DDoS útokom vedeným z externého prostredia. Uvedená skutočnosť je hlavným prínosom článku.

OCA19. - Charakteristika dopadu výstupu a súvisiacich aktivít na vzdelávací proces

Problém riešený vo výstupe (kybernetické útoky a obrana proti nim) má priamy dopad na predmet Informačná bezpečnosť , ktorý je vyučovaný hodnotenou osobou. Problematika riešená vo výstupe priamo zodpovedá náplni tohto predmetu, či už po metodologickej (použité spôsoby útoku a obrany), ale aj technickej stránke (použitý softvér a hardvér) a pozitívne ovplyvní vzdelávací proces. Dopady je možné nepriamo vidieť aj v predmete Projektový manažment .
Navyše bezpečnosť IoT zariadení je témou množstva záverečných prác, ktoré hodnotená osoba v študijnom programe vedie. Rovnako na článok nadväzujú aj zahraničné záverečné práce, napr. : Isah, R. E. (2022). The vulnerability studies and security postures of smart home devices (Master's thesis, Altınbaş Üniversitesi, Turecko). Agarwal, R. (2021). Graph-Based Simulation for Cyber-Physical Attacks on Smart Buildings (Doctoral dissertation, Virginia Tech, USA).

2. hodnotený výstup

OCA5. - Oblasť posudzovania

Aplikovaná informatika

OCA6. - Kategória výstupu tvorivej činnosti

vedecký výstup

OCA7. - Rok vydania výstupu tvorivej činnosti

2018

Charakteristika výstupu, ktorý je registrovaný v CREPČ alebo CREUČ

OCA8. - ID záznamu v CREPČ alebo CREUČ (ak je)

ID = 88263

OCA9. - Hyperlink na záznam v CREPČ alebo CREUČ

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

Charakteristika výstupu, ktorý nie je registrovaný v CREPČ alebo CREUČ

OCA10. - Hyperlink na záznam v inom verejne prístupnom registri, katalógu výstupov tvorivých činností

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

OCA13. - Hyperlink na stránku, na ktorej je výstup sprístupnený (úplný text, iná dokumentácia a podobne)

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

OCA14. - Charakteristika autorského vkladu

Hodnotená osoba sa ako hlavný autor (50 %) podieľala na všetkých fázach tvorby výstupu, od samotného návrhu koncepcie riešenia, cez experimentálne testovanie, analýzu dosiahnutých výsledkov, až po proces písania článku a zapracovanie recenzných odporúčaní. Navyše jeden zo spoluautorov článku bol doktorandom hodnotenej osoby v čase publikovania výstupu.

OCA15. - Anotácia výstupu s kontextovými informáciami týkajúcimi sa opisu tvorivého procesu a obsahu tvorivej činnosti a pod.

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.

OCA16. - Anotácia výstupu v anglickom jazyku

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.

OCA17. - Zoznam najviac 5 najvýznamnejších ohlasov na výstup

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)

OCA18. - Charakteristika dopadu výstupu na spoločensko-hospodársku prax

Článok patrí do radu výskumných úloh riešených v rámci projektu VEGA a APVV zameraných na sieťovú bezpečnosť. Výstup demonštruje zraniteľnosť vybranej skupiny IoT zariadení proti DDoS útokom. Okrem iného článok poukazuje na originálne zistenie, že vo všeobecnosti nie je možné použiť zariadenia IoT na vytvorenie cieleného reflektovaného DDoS útoku na konkrétny počítač obete, ale tento druh útoku má zmysel v konkrétnych situáciách, keď je útok zameraný na veľký počet IP adries smerujúcich cez bežné sieťové pripojenie spôsobom, aby došlo k zahlteniu spojenia.
Hoci sa jedná o konferenčný článok, výstup bol odvtedy citovaný v širokej škále oblastí bezpečnosti IoT zariadení, cez DDoS útoky na IoT zariadenia, budovanie IoT testovacích prostredí, až po reflektovaná DDoS útoky v 5G sieťach.

OCA19. - Charakteristika dopadu výstupu a súvisiacich aktivít na vzdelávací proces

Problém riešený vo výstupe (kybernetické útoky a obrana proti nim) má priamy dopad na predmet Informačná bezpečnosť , ktorý je vyučovaný hodnotenou osobou. Problematika riešená vo výstupe priamo zodpovedá náplni tohto predmetu, či už po metodologickej (použité spôsoby útoku a obrany), ale aj technickej stránke (použitý softvér a hardvér) a pozitívne ovplyvní vzdelávací proces. Dopady je možné nepriamo vidieť aj v predmete Projektový manažment . Navyše bezpečnosť IoT zariadení je témou množstva záverečných prác, ktoré hodnotená osoba v št. programe vedie.

3. hodnotený výstup

OCA5. - Oblasť posudzovania

Aplikovaná informatika

OCA6. - Kategória výstupu tvorivej činnosti

vedecký výstup

OCA7. - Rok vydania výstupu tvorivej činnosti

2021

Charakteristika výstupu, ktorý je registrovaný v CREPČ alebo CREUČ

OCA8. - ID záznamu v CREPČ alebo CREUČ (ak je)

ID = 250414

OCA9. - Hyperlink na záznam v CREPČ alebo CREUČ

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

Charakteristika výstupu, ktorý nie je registrovaný v CREPČ alebo CREUČ

OCA10. - Hyperlink na záznam v inom verejne prístupnom registri, katalógu výstupov tvorivých činností

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

OCA13. - Hyperlink na stránku, na ktorej je výstup sprístupnený (úplný text, iná dokumentácia a podobne)

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

OCA14. - Charakteristika autorského vkladu

Ako je uvedené aj v samotnom článku v časti „Author Contributions“, nosný autorský vklad hodnotenej osoby (40 %) pozostáva pri riešení problému z častí: koncept, metodológia, formálna analýza, samotný výskum, zdroje, písanie - pôvodná príprava konceptu, písanie - recenzia a úpravy, supervízia a získavanie finančných prostriedkov. Navyše jeden zo spoluautorov článku bol doktorandom hodnotenej osoby v čase publikovania výstupu.

OCA15. - Anotácia výstupu s kontextovými informáciami týkajúcimi sa opisu tvorivého procesu a obsahu tvorivej činnosti a pod.

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)

OCA16. - Anotácia výstupu v anglickom jazyku

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.

OCA17. - Zoznam najviac 5 najvýznamnejších ohlasov na výstup

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).

OCA18. - Charakteristika dopadu výstupu na spoločensko-hospodársku prax

Článok predstavuje prípadovú štúdiu, ktorá demonštruje zničujúce účinky útoku DDOS na skutočnú výrobnú linku založenú na IoT a na celý výrobný proces. DDoS útoky na infraštruktúru výrobnej linky sú v literatúre len predpokladané, ale nijak empiricky potvrdené alebo inak doložené. Štúdia vykonaná na reálnej výrobnej linke dokazuje zraniteľnosť infraštruktúry na kybernetické útoky. Článok navyše demonštruje účinnosť navrhnutého obranného riešenia založeného na toku vzoriek (sFlow) z minimálnym dopadom na bežiacu výrobnú linku počas výrobného procesu. Pri článku je sprístupnený aj testovací dataset, ktorý je jedinečný z pohľadu kybernetických DDoS útokov vedených na výrobnú linku.

OCA19. - Charakteristika dopadu výstupu a súvisiacich aktivít na vzdelávací proces

Problém riešený vo výstupe (kybernetické útoky a obrana proti nim) má priamy dopad na predmet Informačná bezpečnosť , ktorý je vyučovaný hodnotenou osobou. Problematika riešená vo výstupe priamo zodpovedá náplni tohto predmetu, či už po metodologickej (použité spôsoby útoku a obrany), ale aj technickej stránke (použitý softvér a hardvér) a pozitívne ovplyvní vzdelávací proces. Dopady je možné nepriamo vidieť aj v predmete Projektový manažment .
Na výstup nadväzuje napríklad spoločná Springer publikácia so študentom bakalárskeho štúdia aplikovanej informatiky zameraná na testovanie DDoS útokov „Comparison of software simulation and network testbed of DDoS attacks for IPv4 and IPv6 networks“.

4. hodnotený výstup

OCA5. - Oblasť posudzovania

Aplikovaná informatika

OCA6. - Kategória výstupu tvorivej činnosti

vedecký výstup

OCA7. - Rok vydania výstupu tvorivej činnosti

2013

Charakteristika výstupu, ktorý je registrovaný v CREPČ alebo CREUČ

OCA8. - ID záznamu v CREPČ alebo CREUČ (ak je)

ID = UCM.Trnava.PC014531

OCA9. - Hyperlink na záznam v CREPČ alebo CREUČ

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

Charakteristika výstupu, ktorý nie je registrovaný v CREPČ alebo CREUČ

OCA10. - Hyperlink na záznam v inom verejne prístupnom registri, katalógu výstupov tvorivých činností

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

OCA13. - Hyperlink na stránku, na ktorej je výstup sprístupnený (úplný text, iná dokumentácia a podobne)

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

OCA14. - Charakteristika autorského vkladu

Hodnotená osoba sa ako hlavný autor (50 %) podieľala na všetkých fázach tvorby výstupu, od samotného návrhu koncepcie riešenia, cez experimentálne testovanie, analýzu dosiahnutých výsledkov, až po proces písania článku a zapracovanie recenzných odporúčaní.

OCA15. - Anotácia výstupu s kontextovými informáciami týkajúcimi sa opisu tvorivého procesu a obsahu tvorivej činnosti a pod.

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

OCA16. - Anotácia výstupu v anglickom jazyku

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.

OCA17. - Zoznam najviac 5 najvýznamnejších ohlasov na výstup

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.

OCA18. - Charakteristika dopadu výstupu na spoločensko-hospodársku prax

Výstup patrí do oblasti informačnej bezpečnosti. V článku je navrhnutý nový autorizačný mechanizmus postavený na princípe dôvery pre ad hoc gridy tak, aby bolo možné ľahšie vytvárať virtuálne organizácie na základe atribútových certifikátov. Výstup je časopiseckým vyvrcholením série konferenčných článkov hodnotenej osoby na uvedenú problematiku v ad hoc gridoch. Výstup významne rozširuje predchádzajúce práce z hľadiska podrobnej formulácie, ako aj validácie navrhovaného bezpečnostného riešenia.
Hoci najväčšie citačné ohlasy na navrhnuté riešenia sú v konferenčných článkoch hodnotenej osoby uvedených v článku [3,9,20], na ktoré hodnotená osoba výstupom nadväzuje, aj na samotný výstup sa odvoláva článok z oblastí MANET sietí.

OCA19. - Charakteristika dopadu výstupu a súvisiacich aktivít na vzdelávací proces

Problém riešený vo výstupe (kybernetické útoky a obrana proti nim) má priamy dopad na predmet Informačná bezpečnosť , ktorý je vyučovaný hodnotenou osobou. Problematika riešená vo výstupe priamo zodpovedá náplni tohto predmetu, či už po metodologickej (použité spôsoby útoku a obrany), ale aj technickej stránke (použitý softvér a hardvér) a pozitívne ovplyvní vzdelávací proces. Dopady je možné nepriamo vidieť aj v predmete Projektový manažment . Navyše bezpečnosť informačných systémov je témou množstva záverečných prác, ktoré hodnotená osoba v št. programe vedie.

5. hodnotený výstup

OCA5. - Oblasť posudzovania

Aplikovaná informatika

OCA6. - Kategória výstupu tvorivej činnosti

vedecký výstup

OCA7. - Rok vydania výstupu tvorivej činnosti

2010

Charakteristika výstupu, ktorý je registrovaný v CREPČ alebo CREUČ

OCA8. - ID záznamu v CREPČ alebo CREUČ (ak je)

ID = UMB.B.Bystrica.0102589

OCA9. - Hyperlink na záznam v CREPČ alebo CREUČ

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

Charakteristika výstupu, ktorý nie je registrovaný v CREPČ alebo CREUČ

OCA10. - Hyperlink na záznam v inom verejne prístupnom registri, katalógu výstupov tvorivých činností

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

OCA13. - Hyperlink na stránku, na ktorej je výstup sprístupnený (úplný text, iná dokumentácia a podobne)

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

OCA14. - Charakteristika autorského vkladu

Hodnotená osoba sa ako hlavný autor (50 %) podieľala na všetkých fázach tvorby výstupu, od samotného návrhu koncepcie riešenia, cez experimentálne testovanie, analýzu dosiahnutých výsledkov, až po proces písania článku a zapracovanie recenzných odporúčaní.

OCA15. - Anotácia výstupu s kontextovými informáciami týkajúcimi sa opisu tvorivého procesu a obsahu tvorivej činnosti a pod.

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.

OCA16. - Anotácia výstupu v anglickom jazyku

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.

OCA17. - Zoznam najviac 5 najvýznamnejších ohlasov na výstup

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)

OCA18. - Charakteristika dopadu výstupu na spoločensko-hospodársku prax

Výstup demonštruje možnosti architektúry CUDA, ktorá využíva výkonnú paralelnú výpočtovú kapacitu GPU na urýchlenie výpočtového procesu odhadu výšky snehovej pokrývky pomocou metódy inverzne váženej vzdialenosti (IDW). Autori riešia problém odhadu snehovej prikrývky v spolupráci s SHMÚ. Na daný výstup nadväzovalo niekoľko ďalších konferenčných a časopiseckých článkov hodnotenej osoby z danej problematiky zameraných na nájdenie vhodného nástroja pre uvedenú problematiku. Hoci sa jedná o konferenčný článok, výstup bol odvtedy citovaný v širokej škále oblastí interpolačných metód a využívania GPGPU.

OCA19. - Charakteristika dopadu výstupu a súvisiacich aktivít na vzdelávací proces

Problém riešený vo výstupe (paralelizácia úlohy, paralelné procesy, programovanie) má nepriamy dopad na predmet Teoretické základy informatiky , ktorý je vyučovaný hodnotenou osobou. A to predovšetkým v druhej časti predmetu venovanej Výpočtovej zložitosti , kde sú preberané triedy výpočtovej zložitosti a možné riešenia výpočtovo náročných úloh. Rovnako sa dopad výstupu odzrkadľuje aj pri zadávaní tém záverečných prác hodnotenej osoby.