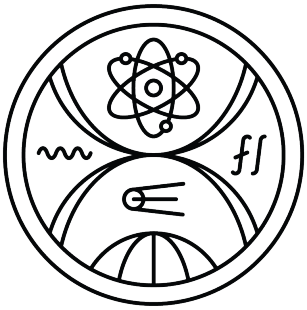
COMENIUS UNIVERSITY IN BRATISLAVA
FACULTY OF MATHEMATICS PHYSICS AND INFORMATICS

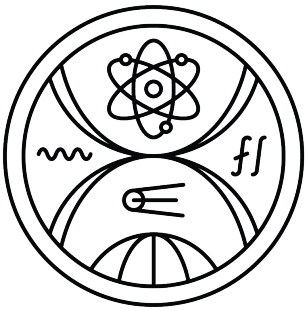


KUBERNETES SECURITY ASSESSMENT

Master thesis

2024 Bc. Pavel Semenov

COMENIUS UNIVERSITY IN BRATISLAVA
FACULTY OF MATHEMATICS PHYSICS AND INFORMATICS



KUBERNETES SECURITY ASSESSMENT

Master thesis

Study program:	Applied informatics
Branch of study:	Applied informatics
Department:	Department of Applied Informatics
Supervisor:	prof. RNDr. Richard Ostertág, PhD.
Consultant:	Mgr. Ľubomír Firment

Bratislava, 2024 Bc. Pavel Semenov

Comenius University Bratislava
Faculty of Mathematics, Physics and Informatics

THESIS ASSIGNMENT

Name and Surname: Bc. Pavel Semenov
Study programme: Applied Computer Science (Single degree study, master II. deg., full time form)
Field of Study: Computer Science
Type of Thesis: Diploma Thesis
Language of Thesis: English
Secondary language: Slovak

Title: Kubernetes security assessment

Annotation: Kubernetes has been gaining popularity rapidly in recent years as more and more enterprise solutions are subjected to cloud transformation and more companies are looking for the ways to increase development efficiency and reduce development costs. This brings new concerns from clients and stakeholders about the security of Kubernetes and its exposure to cyber-attacks.

Aim:

This thesis studies, compares and evaluates the state-of-the-art tools designed to discover vulnerabilities concerning the cluster configuration, running pods or cluster itself. Assessment is carried out in both local cluster setup predisposed with multiple vulnerabilities and real-world enterprise cloud infrastructure. Based on the assessment results we intend either to improve one of the existing tools or develop a Kubernetes security framework of our own, which will be able to provide better results in addressing the cluster security.

Literature:

V. B. Mahajan and S. B. Mane, "Detection, Analysis and Countermeasures for Container based Misconfiguration using Docker and Kubernetes", 2022 International Conference on Computing, Communication, Security and Intelligent Systems (IC3SIS), 2022, pp. 1-6, doi: 10.1109/IC3SIS54991.2022.9885293. https://ieeexplore.ieee.org/document/9885293

D. B. Bose, A. Rahman and S. I. Shamim, "'Under-reported' Security Defects in Kubernetes Manifests", 2021 IEEE/ACM 2nd International Workshop on Engineering and Cybersecurity of Critical Systems (EnCyCriS), 2021, pp. 9-12, doi: 10.1109/EnCyCriS52570.2021.00009. https://ieeexplore.ieee.org/document/9476056

Castillo Rivas, D.A., Guamán, D. (2021). "Performance and Security Evaluation in Microservices Architecture Using Open Source Containers". In: Botto-Tobar, M., Montes León, S., Camacho, O., Chávez, D., Torres-Carrión, P., Zambrano Vizuete, M. (eds) Applied Technologies. ICAT 2020. Communications in Computer and Information Science, vol 1388. Springer, Cham. https://doi.org/10.1007/978-3-030-71503-8_37

Clinton Cao, Agathe Blaise, Sicco Verwer, and Filippo Rebecchi (2022). "Learning State Machines to Monitor and Detect Anomalies on a Kubernetes Cluster". In Proceedings of the 17th International Conference on Availability, Reliability and Security (ARES '22). Association for Computing Machinery, New York, NY, USA, Article 117, 1–9. https://doi.org/10.1145/3538969.3543810

Univerzita Komenského v Bratislave
Fakulta matematiky, fyziky a informatiky

Computing Machinery, New York, NY, USA, Article 117, 1–9. https://doi.org/10.1145/3538969.3543810

Vedúci: RNDr. Richard Ostertág, PhD.
Konzultant: Mgr. Ľubomír Firment
Katedra: FMFI.KI - Katedra informatiky
Vedúci katedry: prof. RNDr. Martin Škoviera, PhD.

Spôsob sprístupnenia elektronickej verzie práce:
bez obmedzenia

Dátum zadania: 07.12.2022

Dátum schválenia: 07.12.2022 prof. RNDr. Roman Ďurikovič, PhD.
garant študijného programu

.....
študent

.....
vedúci práce

I hereby declare that I have written this thesis by myself, only with help of referenced literature, under the careful supervision of my thesis advisor.

.....

Bratislava, 2024 Bc. Pavel Semenov

Acknowledgement

First, I would like to express my gratitude to Mgr. Ľubomír Firment for his guidance during the whole thesis and invaluable expertise in Kubernetes that made this thesis possible. I'd also like to thank my supervisor prof. RNDr. Richard Ostertág, PhD. for his insightful feedback.

Abstract

Kubernetes has been gaining popularity rapidly in recent years as more and more enterprise solutions are subjected to cloud transformation and more companies are looking for the ways to increase development efficiency and reduce development costs. This brings new concerns from clients and stakeholders about the security of Kubernetes and its exposure to cyber-attacks. This thesis studies, compares and evaluates the state-of-the-art tools designed to discover vulnerabilities concerning the cluster configuration, running pods or cluster itself. Assessment is carried out in both local cluster setup predisposed with multiple vulnerabilities and real-world enterprise cloud infrastructure. Based on the assessment results we intend either to improve one of the existing tools or develop a Kubernetes security framework of our own, which will be able to provide better results in addressing the cluster security.

Keywords: kubernetes, security, test, cloud

Abstrakt

Kubernetes v posledných rokoch rýchlo získava na popularite, pretože čoraz viac spoločností hľadá spôsoby, ako zvýšiť efektivitu vývoja a znížiť náklady na vývoj. Táto zvýšená popularita so sebou prináša väčšie vystavenie kybernetickým útokom a zvýšené obavy zainteresovaných strán o bezpečnosť Kubernetes. Cieľom práce je porovnať a zhodnotiť moderné nástroje určené na odhaľovanie zraniteľností týkajúcich sa konfigurácie klastra, bežiacich podov alebo aj samotného klastra. Posúdenie bude prebiehať na lokálnom klastri s prednasadenými viacerými zraniteľnosťami, ako aj v reálnej podnikovej cloudovej infraštruktúre. Na základe výsledkov hodnotenia máme v úmysle buď vylepšiť niektorý z existujúcich nástrojov, alebo vyvinúť vlastný bezpečnostný rámec pre Kubernetes, ktorý bude schopný poskytnúť lepšie výsledky pri riešení klastrovej bezpečnosti.

Kľúčové slová: kubernetes, bezpečnosť, testovanie, cloud

Obsah

Zoznam obrázkov

Zoznam tabuliek

Terminology

Add terms and abbreviations as we encounter them in our text.

Terms

- **Star field tracking (sidereal)**
  Ground-based tracking mode in which, telescope is moving in the same direction and speed as the apparent motion of stars.
- **Object tracking**
  Tracking mode, where the focus is aimed at the moving object of interest and the telescope is moving in the same way.
- **Survey**
  Observation of a region of the sky when no specific target is defined.
- **Star catalog**
  A list of stars with its positions and magnitude.
- **Star tracker**
  An optical device usually used to determine the orientation of satellite using positions of the stars.
- **Deblending**
  The process of separating overlapping objects.

Abbreviations

- **CCD** - Charge-Coupled Device.
- **IAA** - International Academy of Astronautics.
- **USSSN** - US Space Surveillance Network.
- **CNN** - Convolutional Neural Network.
- **FC** - Fully-Connected.
- **RSO** - Resident Space Object.

- **ML** - Machine Learning.
- **SDSS** - Sloan Digital Sky Survey.
- **PCA** - Principal Component Analysis.
- **ANN** - Artificial Neural Network.
- **NN** - Neural Network.
- **MLP** - Multi-Layer Perceptron.
- **R-CNN** - Region-based Neural Network.
- **MS COCO** - Microsoft Common Objects in Context.
- **AGO** - Astronomical and Geophysical Observatory in Modra.
- **AGO70** - The Newtonian telescope at AGO, with 70 cm parabolic mirror.
- **ESA** - European Space Agency.
- **PECS** - Plan for the European Cooperating States.
- **FMPI** - Faculty of Mathematics, Physics and Informatics.
- **FITS** - Flexible Image Transform System.
- **RADEC** - Right Ascension and Declination.
- **FOV** - Field Of View.
- **PSF** - Point-Spread Function.
- **FWHM** - Full Width at Half Maximum.
- **ADU** - Analogue-to-Digital Unit.
- **ADC** - Analog to Digital Converter.
- **SVM** - Support-Vector Machine.
- **ResNet** - Residual Neural Network.
- **ILSVRC** - ImageNet Large Scale Visual Recognition Challenge.
- **RELU** - Rectified Linear Unit.
- **TSV** - Tab-Separated Values.
- **CLI** - Command Line Interface.
- **YAML** - YAML Ain't Markup Language.

Motivation

With a current upward trend in rocket launches and deployment missions, the population of resident space objects has increased rapidly. Due to the imperfections of our technology, we are unable to launch satellites into orbit without leaving behind fragments, rocket bodies and payloads, which gives a rise to the space debris environment. Moreover, more than 30 % of satellites orbiting Earth are no longer functioning . As the space debris population is rising, the need for regular monitoring is essential. The detection of debris allows us to predict its position and actively avoid collisions. It may also help in future missions that aim to collect space debris.

While many solutions to space object detection were already proposed, the majority of them focus on analytical methods. However, the immense amount of data acquired from the space observations, calls for an automatic and more robust technique - machine learning.

In our thesis, we focus on the recognition of astronomical objects with unique features such as streaks, diffuse sources and contaminations on the CCD image. For this purpose, we have designed a convolutional neural network, that classifies images based on the astronomical objects present in them. To train our network with a sufficient amount of data we have implemented a data simulator that generates synthetic astronomical images. The results of our thesis have also been published in the article and presented at the 3rd IAA Conference on Space Situational Awareness.

Literatúra

[1] Convolutional neural network for visual recognition. `https://cs231n.github.io/convolutional-networks/`. Accessed: 25.04.2022.

[2] Introduction to ccd imaging. `https://www.gxccd.com/art?id=303&lang=409`. Accessed: 01.08.2021.

[3] Pytorch documentation. `https://pytorch.org/docs/stable/index.html`. Accessed: 25.04.2022.

[4] S. Andreon, G. Gargiulo, G. Longo, R. Tagliaferri, and N. Capuano. Wide field imaging — I. Applications of neural networks to object detection and star/galaxy classification. *Monthly Notices of the Royal Astronomical Society*, 319(3):700–716, 12 2000.

[5] Olaf Bar, Łukasz Bibrzycki, Michał Niedźwiecki, Marcin Piekarczyk, Krzysztof Rzecki, Tomasz Sośnicki, Sławomir Stuglik, Michał Frontczak, Piotr Homola, David E. Alvarez-Castillo, Thomas Andersen, and Arman Tursunov. Zernike moment based classification of cosmic ray candidate hits from cmos sensors. *Sensors*, 21(22), 2021.

[6] Bertin, E. and Arnouts, S. Sextractor: Software for source extraction. *Astron. Astrophys. Suppl. Ser.*, 117(2):393–404, 1996.

[7] Dr. Michael Bolte. Modern observational techniques: Signal-to-noise in optical astronomy, 2015.

[8] Šolc Brož. *Fyzika sluneční soustavy*, pages 127–133. MatfyzPress, 2013.

[9] Colin J Burke, Patrick D Aleo, Yu-Ching Chen, Xin Liu, John R Peterson, Glenn H Sembroski, and Joshua Yao-Yu Lin. Deblending and classifying astronomical sources with mask r-cnn deep learning. *Monthly Notices of the Royal Astronomical Society*, 490(3):3952–3965, Oct 2019.

[10] Stuart Littlefair Dr. Astronomical techniques, 2015.

[11] Ian Goodfellow, Yoshua Bengio, and Aaron Courville. *Deep Learning*. MIT Press, 2016. `http://www.deeplearningbook.org`.

[12] Don Groom. *Cosmic Rays and Other Nonsense in Astronomical CCD Imagers*, volume 14, pages 81–94. 01 2004.

[13] Kaiming He, Georgia Gkioxari, Piotr Dollár, and Ross Girshick. Mask R-CNN. *CoRR*, abs/1703.06870, 2017.

[14] Kaiming He, Xiangyu Zhang, Shaoqing Ren, and Jian Sun. Deep residual learning for image recognition, 2015. `https://arxiv.org/abs/1512.03385`.

[15] E.P. Hubble. *The Realm of the Nebulae*. The Silliman Memorial Lectures Series. Yale University Press, 1982.

[16] L. Infante and C. J. Pritchet. The CFHT North Galactic Pole Faint Galaxy Survey. *apjs*, 83:237, December 1992.

[17] Heiner Klinkrad. *Space debris: models and risk analysis*. Springer Science & Business Media, 2006.

[18] D. Kyselica, L. Jurkasová, J. Šilha, and R. Ďurikovič. Space objects identification through convolutional neural network algorithms. 04 2022.

[19] Daniel Kyselica. Advanced algorithms for segmentation of space debris astronomical images. Master's thesis, Comenius University, FMPI, 2021.

[20] Yann Lecun, Leon Bottou, Y. Bengio, and Patrick Haffner. Gradient-based learning applied to document recognition. *Proceedings of the IEEE*, 86:2278 – 2324, 12 1998.

[21] Martin Levesque. Detection of artificial satellites in images acquired in track rate mode. 09 2011.

[22] David J. Bell Lisa A. Wells. Cleaning images of bad pixels and cosmic rays using iraf. 09 1994.

[23] Viktor Nagy. Algorithm development for the segmentation of astronomical images with unique features. Master's thesis, Comenius University, FMPI, 2019.

[24] O.Hainaut. Basic image processing. 12 1996.

[25] O.Hainaut. Retouching of astronomical data for the production of outreach images. 05 2009.

[26] Stefan Parimucha and M. Vaňko. Photometry of the variable stars using ccd detectors. i. photometric reduction. *Contributions of the Astronomical Observatory Skalnate Pleso*, 35:35–44, 01 2005.

[27] Pence, W. D., Chiappetti, L., Page, C. G., Shaw, R. A., and Stobie, E. Definition of the flexible image transport system (fits), version 3.0. *A&A*, 524:A42, 2010.

[28] Moonzarin Reza. Galaxy morphology classification using automated machine learning. *Astronomy and Computing*, 37:100492, 2021.

[29] W Romanishin. An introduction to astronomical photometry using ccds. *University of Oklahoma*, 17, 2006.

[30] Olga Russakovsky, Jia Deng, Hao Su, Jonathan Krause, Sanjeev Satheesh, Sean Ma, Zhiheng Huang, Andrej Karpathy, Aditya Khosla, Michael Bernstein, et al. Imagenet large scale visual recognition challenge. *International journal of computer vision*, 115(3):211–252, 2015.

[31] The Europe space agency (ESA). About space debris. `https://www.esa.int/Safety_Security/Space_Debris/About_space_debris`, Accessed: 20.3.2022.

[32] The Europe space agency (ESA). Space debris by the numbers. `https://www.esa.int/Safety_Security/Space_Debris/Space_debris_by_the_numbers`, Accessed: 20.3.2022.

[33] The Europe space agency (ESA). Types of orbits. `https://www.esa.int/Enabling_Support/Space_Transportation/Types_of_orbits`, Accessed: 20.3.2022.

[34] Dario Spiller, Edoardo Magionami, Vincenzo Schiattarella, Fabio Curti, Claudia Facchinetti, Luigi Ansalone, and Alberto Tuozzi. On-orbit recognition of resident space objects by using star trackers. *Acta Astronautica*, 177:478–496, 2020.

[35] J. Šilha, S. Krajčovic, J. Tóth, L. Kornoš, J. Világi, P. Zigo, J. Šimon, D. Kalmančok, M. Hamara, D. Žilková, L. Novák, M. Zigo, F. Ďuriš, V. Nagy, R. Ďurikovič, T. Schildknecht, E. Cordelli, A. Vananti, Ch. Paccolat, and T. Flohrer. Slovakian optical sensor for hamr objects cataloguing and research. 10 2018.