National Aerospace University
«Kharkiv Aviation Institute»

The fourth student scientific and technical conference

STUDENT CONFERENCE INFORMATION, FUNCTIONAL AND CYBERSECURITY (SCIFIC)

November 29 – 30
2024

Kharkiv, Ukraine

INVITATION

The Organizing Committee invites you to participate in the Fourth Student Scientific and Technical Conference «INFORMATION, FUNCTIONAL AND CYBERSECURITY». Postgraduate students, masters' students and students who are doing scientific research in the areas of the conference are invited to participate.

ORGANIZATIONAL COMMITTEE

Conference Co-Chairmen:

Vyacheslav Kharchenko (Doctor of Science on Engineering, Professor, Department of Computer Systems, Networks and Cybersecurity, NAU «KhAI», Kharkiv, Ukraine);

Oles Yudin (PhD student, Department of Computer Systems, Networks and Cybersecurity, NAU «KhAI», Kharkiv, Ukraine).

Organizing Committee:

Volodymir Pevnev (Doctor of Science on Engineering, Associate Professor, Department of Computer Systems, Networks and Cybersecurity, NAU «KhAI», Kharkiv, Ukraine);

Heorhii Zemlianko (PhD in cybersecurity, Department of Computer Systems, Networks and Cybersecurity, NAU «KhAI», Kharkiv, Ukraine);

Yehor Protsenko (student, Department of Computer Systems, Networks and Cybersecurity, NAU «KhAI», Kharkiv, Ukraine);

Daria Herasymiuk (student, Department of Computer Systems, Networks and Cybersecurity, NAU «KhAI», Kharkiv, Ukraine).

LANGUAGES

Communication languages of the conference: Ukrainian, English.

TOPICS

Section 1. Information and cyber security.
Section 2. Functional safety.

IMPORTANT DATES

15 November 2024 - Submission of reports to the Organizing Committee, ready for printing.
29 - 30 November 2024 - Registration of participants and sessions according to the program.

REGISTRATION

Thesis and an application for participation in the conference must be submitted using the Google form: https://forms.gle/enMFBKXUoKbmFPrb6 by *November 15th, 2024*.

Theses are sent in electronic form with the extension: ".doc" or ".docx" and the name according to the template: Surname-Name-Section_(1,2)-Title_of_the_work. (Example: Yudin-Oles-Section_1-Security_IaC).

ORGANIZATION FEE

There are no organizational fees. The proceedings of the conference will be published in electronic form and will have the status of a scientific publication with an ISBN number.
However, if the participant wishes to receive a printed collection of theses, participant must contact with organizing committee. The cost of shipping the printed collection outside of Ukraine is discussed individually with the organizing committee. Payment details can be obtained from the organizing committee by writing to scific@csn.khai.edu.
The organizing committee can ship the collection of theses worldwide ship.
IMPORTANT! The participant must declare his need for printed theses at the same time as sending the abstracts of the report.

CONTACTS

National Aerospace University «Kharkiv Aviation Institute», Department of Computer Systems, Networks and Cybersecurity, ZIP code: 61070, Ukraine, Kharkiv, str. Vadima Manka, 17.
Email: scific@csn.khai.edu

RULES FOR THESIS WRITING

Camera Ready Paper (Thesis) must be 2 pages in A5 format. Thesis should contain references to scientific publications (up to 5 references, not more than 2 are your own publications).
The text editor is MS OFFICE WORD. The page format is A5.
Top margins 1.5 cm, right, left, bottom 2 cm. Font: Times New Roman.
Line spacing – 1.1; Font - 10 pt., straight.
The file name must follow the template: Surname-Name-Section_(1,2)-Title_of_work. (Example: Yudin-Oles-Section_1-Security_IaC).

The first line. Section x (section number).
Starting from the second line: **Report title**: font – bold.
Third line: empty.
From the fourth line, authors: name and surname.
Organization or university: full name of the organization, city, country.
Scientific advisor: name and surname.
Across the line: the main text of the report (in Ukrainian or English language). The text of the report must include the following sections: **relevance**, **purpose**, **principal provisions**, **conclusions**.
First line, indentation – 0.5 cm.
Next line:
References, font: semi-bold, 10 pt. It is possible to use up to five sources and not more than two own publications. The list of sources is prepared in accordance with ДСТУ 8302:2015.
The following is a list of references, 10 pt.
Next line:
Information about the authors (English) – semibold, 10 pt.
Next comes the name, surname, position, department, scientific degree, academic title, contact phone number, e-mail.

An example of report design

Section 1

Research of Security of Infrastructure as a Code Technologies

Oles Yudin
National Aerospace University «Kharkiv Aviation Institute»
Scientific adviser Volodymyr Pevnev

Relevance. With the **growth** of companies providing cloud computing services, tools for definition Infrastructure as a Code (IaC) are gaining popularity rapidly. Modern business is trying to reduce the amount of time spent on deploying applications. After describing the desired project infrastructure, the developer is given the possibility to quickly deploy the environment without performing unnecessary operations with the New IaC approach.

The purpose of this work is to investigate the mechanisms of protection confidentiality of cloud infrastructure, in case of vulnerabilities that arise from an incorrect description of the infrastructure code.

Principal provisions. To timely validation the code for the presence of sensitive information, as well as validation for vulnerabilities inside the software libraries used, it is possible to use special static scanners that will detect vulnerabilities accidentally or intentionally embedded in the source code [3].

Conclusions. The Infrastructure as a Code technology helps flexibly configure and administrate the required project architecture. However, there are abundant threats, part of which are not obvious and need exploring. One of the non-obvious threats is exposing sensitive information from the variable by intercepting network traffic over an unsecured network. The thesis considers the main threats and vulnerabilities in describing IaC technology, which could be profitable and exploited to attack privacy.

List of references

1. Snyk research report, Infrastructure as Code Security Insights. – Snyk. – February 2021.
2. A05:2021 – Security Misconfiguration. OWASP Top 10:2021. URL – https://owasp.org/Top10/A05_2021-Security_Misconfiguration (accessed on 21 July 2022).

Information about the authors

Oles Yudin, a master`s student from the Department of Computer Systems, Networks and Cybersecurity, o.yudin@student.csn.khai.edu
Vladimir Pevnev, Dr. Sc., professor from the Department of Computer Systems, Networks and Cybersecurity, v.pevnev@csn.khai.edu