

STUDENTŲ ĮTRAUKIMO Į MOKSLINĘ VEIKLĄ SKATININAMOJO KONKURSO TEMA

Temos pavadinimas: Dinaminio mikrosegmentavimo Kubernetes aplinkoje pagal „Zero Trust“ principus tyrimas
Tikslas: ištirti kaip mikrosegmentavimas debesų kompiuterijos programų sistemose pagal Zero Trust principą įtakoja programų našumą.
Trumpas temos vykdymo aprašymas (ne daugiau kaip 2000 ženklų): Tradiciškai „Kubernetes“ (K8s) tinklas veikia „plokščiojo tinklo“ principu – pagal nutylėjimą visi konteineriai gali laisvai bendrauti tarpusavyje. Tai visiškai prieštarauja „Zero Trust“. Šiame darbe analizuojama ir kuriama sistema, skirta mikrosegmentavimui – tinklo padalijimui į itin mažus, izoliuotus segmentus (iki atskiro konteinerio lygio). Dinaminis reiškia, kad tinklo apsaugos taisyklės (angl. Network Policies) nėra užrašomos rankiniu būdu vieną kartą visam laikui. Sistema pati, naudodama dirbtinį intelektą ar automatizuotą elgsenos analizę, realiuoju laiku stebi konteinerių elgseną ir automatiškai keičia, sugriežtina arba atlaisvina tinklo prieigos teises.
Temą siūlantis mokslininkas/dėstytojas: Dalius Mažeika

TOPIC OF A COMPETITION PROMOTING STUDENT ENGAGEMENT IN SCIENTIFIC ACTIVITIES

Topic:: A Study of Dynamic Micro-segmentation in a Kubernetes Environment Based on Zero Trust Principles
Goal: To investigate how micro-segmentation in cloud-based application systems, based on the Zero Trust principle, affects application performance.
Short description (max. 2000 characters): Traditionally, Kubernetes (K8s) networking operates on a "flat network" principle, where, by default, all containers can communicate freely with one another. This stands in direct opposition to the "Zero Trust" model. This work analyzes and develops a system designed for micro-segmentation—the division of a network into extremely small, isolated segments (down to the level of an individual container). The term "dynamic" implies that network security rules (Network Policies) are not manually defined once and for all; instead, the system itself—utilizing artificial intelligence or automated behavioral analysis—monitors container behavior in real time and automatically adjusts network access rights, either tightening or loosening them.
Supervisor researcher/lecturer: Dalius Mažeika