UNIVERZITET U SARAJEVU -
ELEKTROTEHNIČKI FAKULTET
S a r a j e v o
Zmaja od Bosne bb

Na osnovu čl. 5. i 6. Odluke Vijeća Univerziteta u Sarajevu - Elektrotehničkog fakulteta o definiranju procedure realizacije naučnoistraživačkih seminara na trećem ciklusu studija - doktorskom studiju (broj: 01-503/21 od 01.02.2021. godine) i Odluke Vijeća Univerziteta u Sarajevu - Elektrotehničkog fakulteta (broj: 01-2369/25 od 07.07.2025. godine), Univerzitet u Sarajevu - Elektrotehnički fakultet, daje

O B A V I J E S T
o odbrani seminara

Studentica trećeg ciklusa studija - doktorskog studija, Amina Tanković, magistar elektrotehnike - diplomirani inženjer elektrotehnike, branit će Naučnoistraživački seminar 2.1. pod naslovom "A Survey on Data Plane Security in Software-Defined Networks: Towards Adaptive Security of Data Planes". Sažetak Naučnoistraživačkog seminara 2.1. se prilaže (objavljuje) uz ovu obavijest.

Seminar je izrađen u saradnji sa akademskim savjetnikom dr.sc. Enijem Kaljićem, vanrednim profesorom Univerziteta u Sarajevu - Elektrotehničkog fakulteta.

Odbrana seminara, održat će se 15. jula 2025. godine (utorak), s početkom u 12:00 sati, u prostorijama Univerziteta u Sarajevu - Elektrotehničkog fakulteta (sala 2-22).

Odbrana seminara je javna.

Obavijest o odbrani i sažetak seminara, oglašavaju se na oglasnim pločama i internet stranici Univerziteta u Sarajevu - Elektrotehničkog fakulteta.

Oglašeno:
Sarajevo, 08.07.2025. godine

Naučnoistraživački seminar 2.1.

Studentica:
Amina Tanković, magistar elektrotehnike - diplomirani inženjer elektrotehnike

Akademski savjetnik:
Dr.sc. Enio Kaljić, vanredni profesor Univerziteta u Sarajevu - Elektrotehničkog fakulteta

"A Survey on Data Plane Security in Software-Defined Networks: Towards Adaptive Security of Data Planes"

Sažetak/Abstract

Engleski:
Software-Defined Networking (SDN) is the actual approach in the network design, based on separating the control and data plane. Such architectural model has brought improvements in terms of network monitoring, management and troubleshooting, but has also increased risks related to network security. Security attacks can occur at all SDN layers and disrupt part or the entire network. Existing research is mostly focused on the security of the control plane, since it contains all control logic of SDN networks and thus represents their main part. Although the data plane has many vulnerabilities and can also be a significant source of security threats towards the control plane, it is only partially covered in existing research, without enough details related to differences between methods and implementation techniques which provide security enhancement. In this paper, we present a comprehensive survey on security of the data plane, focusing on the latest advanced solutions. The survey starts with an overview of attacks, threats and affected security attributes in the data plane, classified using common security models: STRIDE, CIA and AAA. After that, we present a detailed analysis of solutions explored in the literature, including the methods used for security enhancement, implementation techniques, experimental environments, their contributions in terms of vulnerabilities that they address, performance analysis and limitations. Through this analysis, we introduce the concept of adaptive security and select several mechanisms which can be used to achieve it. Additionally, we propose possible combinations of presented mechanisms to provide strong, comprehensive solution which should adapt to dynamics of network, attackers and users, and in that way protect the network from different threats and also satisfy the requirements of services which need different levels of security.

Bosanski:
Softverski definisano umrežavanje (SDN) predstavlja savremeni pristup u dizajnu mreža, zasnovan na razdvajanju kontrolne i podatkovne ravni. Ovakav arhitekturalni model donio je poboljšanja u nadzoru, upravljanju i otklanjanju problema u mrežama, ali je istovremeno povećao rizike povezane sa sigurnošću mreže. Sigurnosni napadi mogu se desiti na svim SDN slojevima i dovesti do poremećaja dijela ili cijele mreže. Postojeća istraživanja uglavnom su fokusirana na sigurnost kontrolne ravni, budući da ona sadrži svu logiku upravljanja SDN mrežama i samim tim predstavlja njihov glavni dio. Iako podatkovna ravan ima mnoge ranjivosti i može biti značajan izvor sigurnosnih prijetnji prema kontrolnoj ravni, u dosadašnjim istraživanjima je samo djelimično obrađena, bez dovoljno detalja o razlikama između metoda i tehnika implementacije koje doprinose unapređenju sigurnosti. U ovom radu predstavljamo sveobuhvatan pregled sigurnosti podatkovne ravni, s fokusom na najnovija napredna rješenja. Pregled započinjemo opisom napada, prijetnji i ugroženih sigurnosnih atributa u podatkovnoj ravni, klasifikovanih korištenjem uobičajenih sigurnosnih modela: STRIDE, CIA i AAA. Nakon toga predstavljamo detaljnu analizu rješenja obrađenih u literaturi, uključujući metode korištene za unapređenje sigurnosti, tehnike implementacije, eksperimentalna okruženja, njihov doprinos u smislu ranjivosti koje adresiraju, analizu performansi i ograničenja. Kroz ovu analizu uvodimo koncept adaptivne sigurnosti i izdvajamo nekoliko mehanizama koji se mogu koristiti za njeno postizanje. Dodatno, predlažemo moguće kombinacije predstavljenih mehanizama kako bi se obezbijedilo snažno, sveobuhvatno rješenje koje se može prilagođavati dinamici mreže, napadača i korisnika, te na taj način štititi mrežu od različitih prijetnji i istovremeno zadovoljiti zahtjeve usluga koje zahtijevaju različite nivoe sigurnosti.