VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA INFORMAČNÍCH TECHNOLOGIÍ

Informace o obhajobě doktorské disertační práce

Ing. Jan Kučera z Ústavu počítačových systémů Fakulty informačních technologií ve středu 11.12.2024 úspěšně obhájil svoji disertační práci.

Studijní program: Výpočetní technika a informatika

Název práce: Flexibilní a událostmi řízená datová cesta/ Flexible and Event-Triggered Data Plane

Abstrakt/Abstract:

Disertační práce se zabývá tématem monitorování a bezpečnosti vysokorychlostních počítačových sítí. Zaměřuje se na optimalizaci aplikací pro bezpečnostní monitorování sítě pomocí programovatelné datové cesty. Využívá specifických vlastností síťového provozu, flexibility programovatelnosti datové cesty a implementuje řadu hardwarových architektur a algoritmů odpovídajících požadovanému zpracování síťového provozu. V rámci práce byl navržen nový koncept flexibilní akcelerace monitorování sítě a detekce škodlivého provozu založený na těžkých tocích, přístup událostmi řízené detekce významných shluků síťového provozu a specifická agregace síťového provozu založená na principu klouzavého okna a extrakce příznaků pro ochranu proti DDoS útokům. Vytvořené architektury využívají pravděpodobnostní datové struktury a techniky pro dosažení vysoké míry úspěšnosti detekce, vysoké propustnosti a nízkých nároků na hardwarové zdroje. Navržené přístupy jsou demonstrovány pro tři různé aplikace: (1) monitorování sítě na bázi síťových toků, (2) vestavěná detekce síťových událostí a (3) potlačení DDoS útoků v reálném čase. Výsledky výzkumu přináší významné zlepšení v oblasti bezpečnostního monitorování sítě. Řízená předfiltrace paketů značně snižuje množství síťového provozu, který musí být nutně analyzován, a dosahuje tak vyšší propustnosti. Přístup založený na událostmi řízené detekci událostí řeší problémy se škálovatelností aplikací a snižuje režii komunikace mezi datovou a řídicí cestou. Ve srovnání s ostatními state-of-the-art přístupy redukuje množství řídicí komunikace o více než dva řády. Představené implementační výsledky práce jsou navíc integrovány jako součást systému DDoS Protector, což je akcelerované řešení ochrany proti DDoS, které bylo jako výsledek výzkumu komercializováno a v současné době chrání českou akademickou síť./ The dissertation thesis deals with the topic of high-speed network monitoring and security. It focuses on optimizing network security monitoring applications using programmable data planes. It exploits the specific network traffic characteristics, the flexibility of network data plane programmability and proposes multiple hardware architectures and algorithms corresponding to the required network traffic processing. The thesis introduces a new concept of flexible heavy flow-based acceleration for network monitoring and intrusion detection, an event-

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ VYSOKÉHO UČENÍ TECHNICKÉHO V BRNĚ
Božetěchova 2, 612 00 Brno
tel.: +420-5-4114 1139, fax: +420-5-4114 1270, http://www.fit.vut.cz

Informace o obhajobě doktorské disertační práce

trigged push-based approach for detecting high-volume traffic clusters, and specific window-based network traffic aggregation and feature extraction, particularly for DDoS defense. The architectures use probabilistic data structures and techniques to ensure high detection performance and throughput with low resource requirements. The investigated concepts demonstrate the network data plane optimizations for three different use cases: (1) the flow-based network monitoring, (2) in-band network events detection, and (3) real-time DDoS mitigation. The research findings brought significant improvements in network security monitoring. Informed packet pre-filtering considerably reduces the amount of network traffic to be analyzed and achieves higher throughput. The event-triggered approach addresses application scalability issues and reduces data-control plane communication overhead. Compared to the other state-of-the-art solutions, the event-triggered approach can save a significant amount of control plane traffic of more than two orders of magnitude. Furthermore, the presented implementation results are utilized in DDoS Protector, an accelerated DDoS protection solution that has been commercialized and protects the Czech academic network.

.

Školitel: doc. Ing. Jan Kořenek, Ph.D., FIT VUT, Česká republika

Oponenti: dr. Tom Barbette, UCLouvain, Belgické království

prof. Ing. Miroslav Vozňák, Ph.D., VŠB, Česká republika