Review of Master's Thesis

Student: Šišmiš Lukáš, Bc.
Title: Optimization of the Suricata IDS/IPS (id 23479)
Reviewer: Fukač Tomáš, Ing., DCSY FIT BUT

1. Assignment complexity — considerably demanding assignment

Zadání práce si vyžadovalo důkladně prostudovat nejen IDS/IPS Suricata ale i systém DPDK a mnoha dalších nízkoúrovňových systémových záležitostí. Kvůli absenci dokumentací systému Suricata a DPDK bylo pro pochopení obou systémů, návrh a implementaci optimalizací nutné důkladně prostudovat zdrojové kódy. Pro realizaci testů bylo dále nutné se seznámit s nestandardními nástroji a zařízeními k tomu potřebných. Z těchto důvodů zadání této práce považuji za značně obtížné.

2. Completeness of assignment requirements — assignment fulfilled

Všechny body zadání byly splněny.

3. Length of technical report — in usual extent

Rozsah předložené technické zprávy je v obvyklém rozmezí a text je často doplněn relevantními obrázky.

4. Presentation level of technical report — 100 p. (A)

Logická struktura práce je na velmi dobré úrovni, jednotlivé kapitoly na sebe logicky navazují, jejich rozsah odpovídá popisované problematice. Text je informačně velmi bohatý a díky názorným obrázkům pochopitelný i pro čtenáře neorientujícího se v dané problematice. V závěru práce je také uvedena úvaha o možnostech dalších optimalizací a vylepšování systému.

5. Formal aspects of technical report — 95 p. (A)

Práce je psaná v anglickém jazyce a obsahuje jen minimum chyb a překlepů. Text práce je obdobně i z typografického hlediska na velmi dobré úrovni, jedinou výtkou je občasné umístění obrázku osamoceně na jednu stranu (např. strany 43, 51).

6. Literature usage — 95 p. (A)

Práce s literaturou je dle citačních zvyklostí a prameny jsou voleny vhodně s ohledem na téma práce. Všechny převzaté prvky jsou odlišeny od autorových. Citace knih by bylo vhodné doplnit i o číslo stránky, že které bylo čerpáno.

7. Implementation results — 90 p. (A)

Realizační výstup spočívá v optimalizaci systému Suricata pomocí volby optimálních parametrů, a především v integrování systému DPDK. Pro automatické testování vlivů jednotlivých parametrů a volbu optimálních bylo vytvořené rozsáhlé testovací prostředí a provedeno velké množství testů. V dalším kroku byl do systému Suricata integrován systém DPDK a pomocí testovacího prostředí byl demonstrován přínos této optimalizace. Všechny realizační výstupy jsou plně funkční. Zdrojové kódy by však mohly být lépe komentovány.

8. Utilizability of results

V rámci práce byly navrženy optimální konfigurační parametry systému Suricata, který byl dále rozšířen o podporu DPDK. Přidání této podpory snižuje výkonové nároky spojené s režií kopírování paketů a tím urychluje jejich příjem a zpracovávání. Realizační výstup je plně funkcí a plně připraven pro nasazení na vysokorychlostní sítě. Vytvořené testovací prostření umožňuje automatizovaně testovat propustnost systému a jednoduše tak testovat další optimalizace. Dosažené výsledky byly pravidelně prezentované výzkumné skupině ANT a doporučuji je prezentovat na konferenci Suricon 2021.

9. Questions for defence

- V grafu na obrázku 3.12 je drop rate pro některé testy od určité rychlosti konstantní, přesto že je očekáván neustálý nárůst (např. varianty se dvěma replikacemi bez shuntingu od rychlosti cca 16 Gb/s). Čím je to způsobeno?

10. Total assessment

95 p. excellent (A)

Student se i přes značnou obtížnost zadání problému zhostil velmi svědomitě, což se odrazilo na velmi kvalitním návrhu a implementaci optimalizací a také na textu technické zprávy. Práce dosahuje velmi zajímavých výsledků, které jsou pro praxi přínosné a použitelné. Dosazené výsledky jsou navíc podloženy řadou testů. Text práce je možné také použít jako návod pro integraci dalších modulů a rozšíření. Pro celkové hodnocení práce proto navrhuji stupeň **A - výborně** a doporučuji udělení **ceny děkana**.

In Brno 3 June 2021

Fukač Tomáš, Ing.
reviewer