# Posudek diplomové práce

*předložené na Matematicko-fyzikální fakultě*
*Univerzity Karlovy v Praze*

## Název práce:

Integrated Network Traffic Processing Framework

## Autor práce:

Tomáš Hrubý

## Posudek oponenta:

Diplomová práce pana Hrubého se zabývá problémem monitorování a filtrování síťového provozu ve vysokorychlostních sítích, což je nutné nejenom k zajištění dohodnuté kvality poskytovaných služeb, ale také k obraně proti nejrůznějším typům útoků zaměřeným na uživatelské stanice a síťovou infrastrukturu. Vzhledem k rychlému vývoji síťových technologii začíná být monitorování a filtrování síťového provozu za hranicemi možností běžného hardware. Proto je nutné nasazení specializovaných zařízení a jejich integrace do existujících i nově vznikajících monitorovacích a filtrovacích nástrojů. Autor ve své práci popisuje návrh a implementaci podpory specializovaného síťového procesoru řady IXP24xx jako akcelerátoru v kontextu obecného paketového filtru FFPF a také jako výkonného jádra síťového zařízení provádějícího filtraci a transformaci paketů na základě pravidel zapsaných v jazyce Ruler.

Ve spojení s paketovým filtrem FFPF autor zobecnil a rozšířil koncept flowspaces na více úrovní než rozlišovala původní implementace, což umožnilo implementaci filtrů na síťovém procesoru. Při rozšiřování FFPF bylo nutné vyřešit celou řadu technických problémů týkajících se umisťování filtrů do flowspaces, správě paměti a front paketů a přenosu dat mezi síťovým procesorem a hostitelským systémem. Ve spojení s jazykem Ruler autor implementoval back-end překladače, který produkuje kód pro paralelní běh na mikrojádrech síťového procesoru. V tomto případě bylo nutné řešit problémy týkající se vícevláknového zpracování paketů a s tím související synchronizace, hledání vzorů v datových tocích a nikoliv pouze v jednotlivých paketech a v neposlední řadě i zohlednění paměťové hierarchie síťového procesoru v generovaném kódu.

Nejsilnější stránkou práce jsou bezpochyby technické informace týkající se řešení uvedených problémů a programovacích technik s ohledem na použitý síťový procesor. Rovněž považuji za nutné vyzdvihnout zpracování práce v angličtině, publikaci výsledků práce ve sborníku mezinárodní konference a celkovou použitelnost výsledků práce i na „běžné" aplikace jako např. detekci průniků do sítě s využitím báze pravidel projektu Snort.

S vysokou technickou úrovní práce pak poněkud kontrastuje slabší zpracování textové části, přičemž hlavním problémem je podle mého názoru nedostatek nadhledu a z toho vyplývající nedostatečné oddělení popisu technických a implementačních detailů od popisu architektury a abstraktnějších konceptů. Při popisu výkonnosti systému by pak bylo vhodné prezentovat podrobnější údaje a alespoň základní statistické veličiny.

Celkově práci chybí zavedený vzor psaní ve stylu kontext-problém-řešení, kde by autor nejprve představil základní koncepty, poté identifikoval konceptuální a technické problémy související s vytyčenými cíli a nakonec popsal jejich řešení. Jako příklad bych uvedl kapitolu 2, kde se v textu mísí popis původní a nové architektury paketového filtru FFPF a kde se na stejné úrovni píše o konceptech jako je flowspace či flowgrabber (které navíc tou dobou ještě nebyly dostatečně popsány) a zároveň o některých technických detailech řešení.

I přes výhrady ke zpracování textové části jsem však toho názoru, že kvalitě práce dominují především její silné stránky, a že uvedené slabiny představují spíše vadu na kráse než závažný problém. Závěrem konstatuji, že práce vyhovuje požadavkům na ni kladeným, a proto ji doporučuji k obhajobě.

V Praze, 30.1.2007

Lubomír Bulej