



## Posudek vedoucího diplomové práce

Jméno studenta: Bc. Martin VACH

Téma práce: Paketový filtr a modifikátor

Cíle práce: V teoretické části bude popsána podpora filtrování a modifikování paketů operačních systémů Linux (od jádra verze 2.6 po současné) a Windows (od verzí XP a Server 2003 po současné). Dále bude vytvořen přehled nástrojů umožňujících na těchto systémech zachytávat, filtrovat a modifikovat pakety.

V praktické části bude navržen a implementován nástroj (program) pro filtrování a modifikování paketů na platformách Windows (nástroje mohou být různé pro různé verze systémů, protože dostupná podpora se liší). API nástroje bude podporovat zahrnutí vlastního filtrovacího kódu pro modifikaci paketů protokolu IP. Uživateli-programátorovi se předá každý paket ke zpracování (a případné modifikování), zpět nástroji bude předán také příznak, zda se má paket propustit nebo zahodit. Paketový filtr bude otestován na zadané aplikaci.

### 1. Uplatnění metod (příslušejících navazujícímu magisterskému studiu)

Student vypracoval přehled dostupných prostředků pro filtrování a modifikace paketů na platformách Windows a Linux dle zadání. Na základě vyhodnocení prostředků pak navrhl a implementoval filtrovací a modifikační nástroj pro platformu Windows (WFP). Úroveň potřebných znalostí převyšuje znalosti vyžadované na navazujícím magisterském studiu.

### 2. Produkt vytvořený při vypracování DP

Byla navržena a vytvořena aplikace skládající se z ovladače pro systémy Windows (7, 8 a 8.1) a uživatelského filtru.

### 3. Prokázání správnosti navrženého řešení problému

Vytvořený ovladač umožňující modifikovat pakety i příslušný paketový filtr byly úspěšně otestovány v demo-aplikaci i v dané aplikaci vyžadující zachycení paketů UDP a jejich modifikaci dle analýzy obsahu dat..

### 4. Naplnění uložených cílů

Cíle byly všechny splněny.

### 5. Kvalita textu z hlediska jeho struktury, srozumitelnosti, jazykové a typografické úrovně

Práce je logicky členěna vhodně do kapitol, které na sebe logicky navazují.

V textu je však mnoho chyb od překlepů, přes chybějící či přebývající čárky, zaměňované pomlčky a spojovníky, nečeské uvozovky, nesprávné koncovky, až po nepřesnosti v pojmech (např. prezenční × prezentační vrstva – obr. 1.1, ENC × ECN – str. 34, data × jejich reprezentace – str. 41). Není zapnuto dělení slov, což vede na mnoha místech k nevhodnému rozpálení řádků, kdy mezilovňní mezery jsou příliš velké.

Seznam zdrojů neodpovídá platné citační normě ISO ČSN 690:2011. Práce s citacemi je na dobré úrovni, přesto však některé informace nelze jednoduše ověřit dle zdroje, neboť je odkazována pouze hlavní stránka projektu (zdroj [6]) místo odkazů na příslušné nástroje. V příslušné části textu (kapitola 3) se vyskytuje řada nepřesností (pojem klasifikátor – str. 33, akce DROP pro nevyhovující pravidla – str. 34, řetězec OUTPUT pro pakety opouštějící uzel – str. 34, libnetfilter-queue × NFqueue – sekce 3.1.3 a 3.1.4 – NFqueue je prezentován jako další prostředek, přičemž se jedná stále o tentýž).

## **6. Nejasnosti v DP, které je třeba objasnit při obhajobě, a doplňující otázky**

Na základě zkušeností získaných při studiu materiálů a implementaci (uživatelského) paketového modifikátoru se pokuste srovnat dostupnou podporu systémů Windows a Linuxu.

Pokuste se přiblížit problematiku s podepisováním ovladače pro systémy Windows v souvislosti s možným šířením výsledného produktu DP.

**Doporučení k obhajobě:**

**ano**

**Navržený klasifikační stupeň:**

**velmi dobře**

**Posudek vypracoval(a):**

Jméno, tituly: Mgr. Tomáš Hudec

Zaměstnavatel: UPa, FEI, KIT

V Pardubicích dne 29. 8. 2014

Podpis: .....