Posudek diplomové práce

Bc. Martin Petrák: Softwarový firewall pro filtrování na síťové a linkové vrstvě

Diplomant měl ve své práci za úkol seznámit se s problematikou filtrování síťového provozu a měl porovnat existující možnosti pro filtrování na síťové a linkové vrstvě. Na tomto základě měl navrhnout architekturu univerzálního SW firewallu pro filtrování provozu v režimu přepínače a směrovače. Navržené řešení měl ověřit implementací grafického rozhraní pro konfiguraci firewallu a zobrazování stavu.

V úvodu diplomant rozebírá obecnou počítačovou bezpečnost, především pak útoky na počítačové sítě zvenku. Klade si za cíl vytvořit filtrovací program pro usnadnění práce administrátorům počítačových sítí.

V kapitole č. 2 diplomant rámcově popisuje principy paketových filtrů. Čerpal převážně z jediné publikace, textu chybí pohled z více úhlů a návaznost. Bez definic pojmů se předpokládá znalost ISO/OSI modelu, který je však rozebrán až v následující kapitole. ISO/OSI model je popsán detailně a diplomant správně poznamenává, že se jedná pouze o teoretický model a v současných sítích jsou některé vrstvy sloučené.

V kapitole č. 4 diplomant popisuje typy protokolů linkové a síťové vrstvy se zaměřením na nejrozšířenější protokoly Ethernet a IP. Zaměřil se také na problematiku fragmentace IP paketů a možnosti útoků, ale bylo by vhodné text obohatit o konkrétní příklady.

V kapitole č. 5 diplomant srovnává několik možných implementací síťových filtrů pro OS Linux a pro další práci správně volí nejrozšířenější implementaci Netfilter. Netfilter je následně velmi detailně popsán. Míra detailů je zbytečně velká, v implementaci SW firewallu je využito minimum těchto informací.

Od kapitoly č. 7 dále diplomant popisuje návrh a implementaci SW firewallu. Text je bohužel více koncipován jako příručka programování s knihovnou Qt v příkladech než jako rozbor potřeb a návrh řešení moderního intuitivního SW firewallu. Ani výsledný program v podstatě nenabízí nic víc než přímočarý převod obsahu vstupních polí do ovládacích příkazů Netfilteru, práce administrátorů tak není ušetřena.

Kvalita typografie diplomové práce je průměrná. V obsahu jsou zahrnuty všechny úrovně kapitol, je velmi dlouhý. Téměř všude chybí tvrdé mezery za jednoznakovými předložkami a spojkami. Všechny obrázky a diagramy jsou rastrové s nízkým rozlišením, texty jsou v nich špatně čitelné. U přejatých obrázků chybí citace.

Doporučuji, aby diplomant během obhajoby zodpověděl následující otázku: Jaké výhody má Vaše řešení oproti podobnému programu ufw (Uncomplicated Firewall, https://launchpad.net/ufw) s velmi jednoduchým grafickým rozhraním, nebo programu firehol (http://firehol.sourceforge.net/), který sice nemá GUI, ale nabízí v konfiguraci vyšší míru abstrakce pravidel?

Volím známku **dobře** a doporučuji k obhajobě.

Ing. David Široký
Plzeň, 3. 6. 2013

SOUHLASÍ
S ORIGINÁLEM

Západočeská univerzita v Plzni
Fakulta aplikovaných věd
katedra informatiky a výpočetní techniky