Věc: **Posudek tezí disertační práce Mgr. Jana Vykopala „Flow-based Intrusion Detection in Large and High-Speed Networks“**

Předmětem posudku je materiál označený „Flow-based Intrusion Detection in Large and High-Speed Networks“, PhD Thesis Proposal, tedy návrh tezí disertační práce. Návrh tezí autor rozčlenil do tří kapitol a doplnil o přehled svých hlavních výsledků v oblasti publikační, presentační, účasti na projektech a výukové včetně vedení prací studentů. Kromě toho přiložil kopie vybraných pěti článků, obsahujících původní výsledky. Teze jsou předkládány současně i jako rigorózní práce. Rozsah práce je 24 stran plus uvedené kopie článků.

První částí práce je úvod, kde autor stručně pojednává o problematice detekce průniku a vysvětluje podstatu detekce průniku založené na zkoumání toků (Flow-based Intrusion Detection, resp. Network Behaviour Analysis, NBA). Popisuje i podstatu slovníkových útoků.

Ve druhé kapitole seznamuje s aktuálním stavem ve zkoumané oblasti a uvádí některé důležité definice, zejména pojmu tok (flow). Detailněji rozvádí problematiku protokolu NetFlow a jeho implementace, ukazuje na související okolnosti, možnosti získávání a zpracování dat atd. Zvláštní pozornost věnuje specializovaným sondám. Dále diskutuje možnosti ukládání a zejména analýzy získaných dat s ohledem na zjišťování anomálií. Specifikuje rovněž některé používané nástroje jak komerční, tak i volně dostupné a objasňuje jejich možnosti s ohledem na NBA. Uvádí vybrané metody jako je porovnávání signatur a vhodně se odkazuje na poznatky jiných autorů. Konečně se zabývá možnými způsoby prezentace získaných výsledků, kde situace dosud neustálená, zejména ohledně vizualizace útoků. V neposlední řadě popisuje varianty detekce slovníkových útoků, zejména s ohledem na SSH. Zde uvádí možnost statistické analýzy pro zjištění útoků. V závěru kapitoly charakterizuje oblast NBA jako pasivní metodu detekce průniku pracující s toky, v čase blízkém reálnému, a to na síťové a transportní vrstvě TCP/IP modelu; architekturu NBA popisuje jako čtyřsložkovou. Rovněž sumarizuje úvahy o detekci slovníkových útoků.

Ve třetí kapitole shrnuje cíle svého výzkumu, jde jednak o problematiku detekce průniku pomocí toků a to v prostředí vysokorychlostních sítí, zejména s ohledem na detekci slovníkových útoků. Konstatuje, že za tímto účelem byla navržena řada algoritmů, které byly prakticky ověřeny a předpokládá se jejich implementace do systémů monitorujících provoz v síti Masarykovy univerzity. Kromě jiného se jednalo o metody detekce zařízení, provádějících překlad adres. V závěru této kapitoly uvádí konkrétní plán své další práce, odevzdání disertační práce předpokládá na podzim roku 2011, její obhajobu pak na jaře 2012.

Stanovisko k předloženému návrhu tezí: je zřejmé, že Mgr. Jan Vykopal má v řešené oblasti i v oblastech souvisejících vynikající přehled, praktické zkušenosti a zejména potřebné tvůrčí i organizátorské schopnosti. Domnívám se, že předložený návrh tezí je zpracován kvalitně. Navržená práce má jasně a reálně stanovené cíle, očekávané výsledky lze považovat za disertabilní a v zamýšleném termínu mohou být reálně dosažitelné. Domnívám se, že teze v daném pojetí lze akceptovat jako rigorózní práci.

V Brně, 30. března 2010

Ing. Josef Kaderka, Ph.D.
Univerzita obrany
Fakulta vojenských technologií
Katedra komunikačních a
informačních systémů

kade@unob.cz
973442704