Oponentní posudek disertační práce

Autor: Ing. Matej Kačic

Název: Analýza útokov na bezdrôtové siete

Vydavatel: Vysoké učení technické v Brně, Fakulta informačních technologií, Ústav inteligentních systémů

Zpracovatel posudku: doc. Ing. Jaroslav Dočkal, CSc., Vysoká škola Karla Engliše, a.s., Ústav informatiky

Námět práce zcela odpovídá oboru disertace a je aktuální z hlediska současného stavu vědy. Problematika bezpečnosti bezdrátových sítí je dlouhodobě problémovým článkem současných počítačových sítí.

Práce vykazuje původní přínosné části, a to ve dvou směrech: systém pro generování běžnými dosavadními prostředky nedetekovatelných útoků (injekce škodlivého kódu do prostředí bezdrátové sítě) a architektury systému pro analýzu anomálií a útoků pomocí principu výpočtu důvěry a reputace, kterýžto cíl práce byl autorem označen jako hlavní. Originální přínos práce spočívá v návrhu systému pro analýzu zranitelností a útoků na bezdrátové sítě. Jako způsob hodnocení jednotlivých zařízení byl vybrán princip založený na výpočtu důvěry a reputace – podkapitola 6.4.5 až 6.4.6, abstraktní algoritmus fungování systému je obsahem podkapitoly 6.5 a potřebný datový model obsahem kapitoly 6.6.

Pro provedení potřebných experimentů bylo třeba navrhnout systém pro generování útoků. Syntax jazyka použitého k popisu rámců a manipulaci s nimi vychází z jazyka použitého k popisu paketů v programu Scapy, což je poměrně logická volba pro relativní jednoduchost řešení ve srovnání s dalšími alternativami (podkapitola 3.4), navíc je free. V kapitole 4 je provedena analýza útoků s dopadem na dostupnost. Pozitivně hodnotím vytvoření prostředí pro demonstraci útoků a jejich experimentální provedení, konkrétně RTS flood útoku (podkapitola 4.1.3) a CTS flood útoku (podkapitola 4.1.4).

Samy experimenty jsou předmětem kapitoly 7 – byl zpracován přehled metrik používaných jinými autory (viz tabulka 7.2 – v samostatném sloupci bylo vhodné uvést, od kterého autora je která metrika, hromadné odkazování na zdroje není vhodné), byly rovněž navrženy vlastní metriky a ty byly posuzovány z pohledu detekčního potenciálu a stability hodnoty důvěry. Vhodnost použití jednotlivých metrik pro výpočet důvěry je přehledně uveden v tabulce 7.4. Autor prokázal schopnost vlastní tvůrčí vědecké práce.

Systém generování útoků měl jako parametry stanovenou jednoduchost a téměř neomezená možnost experimentů nad sítěmi podle standardu 802.11. Útok byl definován pomocí pseudojazyka. Pro příklad analýzy byla vybrána zranitelnost „Hole 196“ (2010). Systém měl být lehce rozšiřitelný a zároveň jednoduchý na pochopení, což jsou samozřejmě relativní pojmy, pokud se neprovede porovnání.

Domnívám se, že úvodní části práce mohly být více řešeny odkazy na dostupné zdroje a nebylo třeba vše v práci uvádět (např. co je FHSS a DSSS). Autor mohl vynechat popis protokolů transportní vrstvy a předpokládat, že zájemce o jeho práci tuto znalost asi bude mít, pro případ výjimky bylo možné použít odkazy na dostupnou literaturu. Text nemusel tudíž být tak obsáhlý, u obsáhlejších textů se totiž nelze vyhnout překlepům, zde viz např. „injeckia rámcov“, či špatným formulacím, viz např. „zranitelnost TKIP algoritmus Michael“ (str. 23). Ocenil bych v řadě méně neurčitá a více jednoznačnější vyjadřování, např. různé

„zaoberování sa“ (str. 6, 7, 12, 24, 28, 43, 53, 54, 67, 86. 98, 109), pro příklad dále uvedu segment věty ze str. 51: To čo chýbá v každej z těchto prác“ – je míněno jako „To čo podľa mňa chýba v každej z týchto prác“? Dále se podle mne do vědecké práce příliš nehodí termín „sofistikovaný“ (str. 90 a 109). Celkově ale jde o výtky formální a nedotýkající se kvality vlastní vědecké práce.

Jádro disertační práce bylo publikováno na potřebné úrovni. Ze seznamu vědecké činnosti uchazeče vyplývá, že se jedná o pracovníka s vědeckou erudicí. V seznamu publikací je uvedeno 13 zdrojů, z toho 10 vydaných v renomovaných zahraničních nakladatelstvích, dvě ve sbornících prestižních tuzemských konferencí a jedna v odborném časopise DSM, což osobně kvituji rovněž velmi pozitivně. 12 z 13 publikací je se spoluautory, zde bych čekal uvedení autorského podílu (stačí odhad), to ovšem lze doplnit v rámci obhajoby práce.

K tištěné verzi práce je (doslova) přilepeno CD, které, jak předpokládám, obsahuje přílohy práce. Samo o sobě je to pozitivní, ovšem v úvodu práce by mělo být uvedeno, co na CD je, a s těmito přílohami v textu práce nějakým způsobem pracovat.

Závěr: Podle mého názoru disertační práce uchazeče odpovídá obecně uznávaným požadavkům k udělení akademického titulu.

….

V Brně 30. června 2018