Technická univerzita v Košiciach, Fakulta elektrotechniky a informatiky

HODNOTENIE HABILITAČNEJ PRÁCE

POSUDOK OPONENTA PRÁCE

Názov práce: **Vybrané metódy detekcie prienikov s využitím lákadiel**

Autor: **Ing. Eva Chovancová, PhD.**

Odbor habilitačného konania a inauguračného konania: ***Informatika*** Akad. rok: ***2019/2020***

Oponent: **doc. Ing. Pavel Segeč, PhD.**

Pracovisko oponenta: ***Žilinská univerzita v Žiline***

KOMENTÁR OPONENTA HABILITAČNEJ PRÁCE

OPONENTSKÝ POSUDOK HABILITAČNEJ PRÁCE
Ing. Evy Chovancovej, PhD.
„Vybrané metódy detekcie prienikov s využitím lákadiel“

Habilitačná práca Ing. Evy Chovancovej, PhD. je venovaná téme informačnej bezpečnosti zameranej na problematiku detekcie sieťových bezpečnostných prienikov s využitím lákadiel, tzv. honeypot-ov. Tému informačnej bezpečnosti v súčasnom stave globálnej konektivity a aktuálneho vývoja v oblasti útokov/hrozieb a obrany považujem za veľmi aktuálnu a naberajúcu čoraz väčší význam a samostatnosť vo výskume ako aj pri riešení prevádzky IKT systémov. Na Slovensku s nástupom zákonných noriem v oblasti kybernetickej bezpečnosti aj s reálnym dopadom. Pri vypracovaní posudku som čerpal z predloženej práce a podkladov, poskytnutých fakultou FEI TUKE.
Predložená práca má celkovo 167 strán, vrátane zoznamu vlastných aj analyzovaných literárnych zdrojov. Pri vypracovaní práce autorka použila bázu 101 referenčných zdrojov. Predložená práca je koncipovaná ako súbor publikovaných vedeckých prác, ktorých je habilitantka autorkou či spoluautorkou. Ten je doplnený komentárom. Tomuto zodpovedá forma a metódy spracovania. Práca je rozdelená do úvodu, troch číslovaných kapitol a záveru.
Z hľadiska štruktúry sa autorka v prvých dvoch kapitolách venuje teoretickému úvodu a orientácii v problematike kybernetickej bezpečnosti. Prvá kapitola v rozsahu 10 strán ponúka štruktúrovaný úvod do zvolenej problematiky v oblasti informačnej bezpečnosti, bezpečnostných hrozieb a základných prvkov implementácie zabezpečenia. Obsiahlejšia 19-násť stranová druhá kapitola sa zameriava už len na systém „Honeypot/lákadlo“ ako bezpečnostný nástroj, pričom popisuje princíp fungovania týchto systémov, kategorizáciu a delenie, prínos v oblasti bezpečnosti IKT technológií. Štruktúra a spracovanie je prehľadné, rozsah analyzovaných zdrojov je obsiahly, prevažne vo forme kníh.
Dosiahnuté výsledky autorky a hlavná časť práce je prezentovaná v tretej kapitole. Kapitola 3 pozostáva z výberu deviatich publikovaných prác vo zvolenej problematike habilitačnej práce, ktorej odpovedá práve deväť kapitol uvedených komentárom. Kapitolu 3 je však možné logicky rozdeliť do dvoch oblastí výskumu bezpečnosti, a to:

- Oblasť 1: detekcia prienikov s využitím lákadiel.
- Oblasť 2: vývoj v oblasti zberu a agregácie dát v sieťovom prostredí.

Do prvej oblasti sa radí sedem publikácií. Autorkin výskum v nich postupne smeruje od autonómnych riešení k návrhu a implementácii architektúry sofistikovaného klastrového hybridného lákadla. Riešenie využíva lákadlá s rôznou interakciou a autonómiou zasadených v rámci systémov detekcie prienikov, pričom sa autorka zameriava aj na efektivitu z hľadiska spravovania samotných lákadiel.
Druhá oblasť výskumu autorky, tvorená dvomi publikáciami, sa venuje oblasti monitoringu, zberu dát v sieťovej prevádzke a jeho optimalizácií týchto činností. Tu sa autorka a kolektív zameriava na zefektívnenie metód vzorkovania sieťového toku cez adaptabilné vzorkovanie sieťového toku či agregáciu nazbieraných hodnôt.
Predložený súbor prác vznikol ako súčasť viacročných výskumných aktivít autorky v rámci riešenia výskumných úloh projektov VEGA (1), KEGA (1) a APVV (2). Súbor prác predstavujú práce publikované v domácich karentovaných časopisoch (2), zahraničných recenzovaných zborníkoch (4), zahraničných časopisoch (1) a zborníkoch z domácich medzinárodných konferencií (1). Kladne hodnotím, že výskum vo vybraných oblastiach viedol práve k spomínaným karentovaným publikáciám. Zaradené publikácie, a najmä tie karentované, ponúkajú prínosné výsledky v oblasti detekcie prienikov s použitím lákadiel a optimalizácie zberu údajov s využitím adaptívnej agregácie sieťového toku. Predkladaná práca poskytuje prehľad výskumu autorky v rokoch 2009 až 2020 a jasne poukazuje na aktívnu profiláciu autorky, ktorej výskumná práca prispieva k rozvoju bezpečnosti v oblasti detekcie prienikov s využitím lákadiel.
Práca je napísaná prehľadne a zrozumiteľne. Formálne aj obsahovo je primerane členená. Mala pripomienka, publikáciu „A Clustered Hybrid Honeypot Architecture“ som nenašiel v zozname zdrojov.
Vo vedeckej činnosti sa habilitantka dlhodobo venuje problematike bezpečnosti so zameraním na využívanie honeypot-ov v detekcií bezpečnostných útokov a sledovania správania útočníkov. Tomu odpovedá aj publikačná činnosť autorky, ktorá z celkovo 65 záznamov obsahuje 15 zameraných na oblasť lákadiel. Celkovo za oblasť VaV činnosti konštatujem naplnenie habilitačných kritérií, s uznaním výstupov a činnosti autora v slovenskej aj medzinárodnej odbornej komunite (WoS/Scopus), čomu zodpovedá aj štruktúra ohlasov na jednotlivé vedecko-výskumné výstupy.
V oblasti pedagogickej činnosti autorka 11 rokov vedie cvičenia viacerých predmetov, ktoré súvisia s predmetom jej výskumu. Habilitantka je autorkou jednej VŠ učebnice a jedného skripta. Viedla 66 záverečných prác, bola zapojená do riešenia 2 KEGA projektov a 2 univerzitných projektov zameraných na oblasť vzdelávania. Jej pedagogické aktivity považujem za primerané a prispievajúco k výchove študentov v odbore.
K téme predloženej habilitačnej práce mám nasledujúce otázky:

- V oblasti detekcie prienikov sa autorka venuje nástroju lákadlo pričom uvádza ich rôzne typy, môže autorka stručne popísať bližšie ich rozdiely ?
- Môže autorka uviesť hlavné výhody a nevýhody lákadiel pri použití v oblasti detekcii prienikov? Aké je ich využívanie v súčasných bezpečnostných riešeniach?
- Stretla sa autorka s nasadením lákadiel v oblasti bezpečnosti cloud-ov? Je tu nejaká možnosť ich využitia?

Na základe celkového zhodnotenia predloženej práce, VaV či pedagogických aktivít, ako aj naplnenia habilitačných kritérií konštatujem vysokú odbornú a pedagogickú úroveň habilitantky v predmetnej oblasti. Preto odporúčam habilitačnej komisii a Vedeckej rade Fakulty elektrotechniky a informatiky TU v Košiciach vymenovať Ing. Evu Chovancovú, PhD. za

docenta
v odbore habilitačného konania: Informatika.
Žilina, 16.9.2020

doc. Ing. Pavel Segeč, PhD.
Katedra informačných sietí
FRI UNIZA

Predloženú habilitačnú prácu na základe predchádzajúceho hodnotenia

ODPORÚČAM prijať k obhajobe

a po jej obhájení navrhujem udeliť vedecko-pedagogický titul "docent (doc.) v odbore "

Dátum: 17.09.2020 .....
podpis autora posudku