Technická univerzita v Košiciach, Rektorát

HODNOTENIE HABILITAČNEJ PRÁCE

POSUDOK OPONENTA PRÁCE

Názov práce: **Vybrané aspekty a metódy systémov detekcie prienikov v oblasti bezpečnosti sieťovej komunikácie**

Autor: **Ing. Martin Chovanec, 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

Habilitačná práca Ing. Martina Chovanca, PhD. je venovaná téme sieťovej bezpečnosti zameranej na problematiku vybraných aspektov a metód detekcie sieťových prienikov. Téme veľmi aktuálnej a neustále napredujúcej, ktorá sa stáva časťou s čoraz dôležitejším vplyvom na prevádzku IKT systémov. Pri vypracovaní posudku som čerpal z predloženej práce a podkladov, poskytnutých fakultou FEI TUKE.

Predložená práca má celkovo 178 strán vrátane vlastných aj analyzovaných literárnych zdrojov. Pri vypracovaní práce autor analyzoval širokú bázu 146 referenčných zdrojov. Predložená práca je koncipovaná ako súbor publikovaných vedeckých prác doplnený komentárom, čomu zodpovedá forma a metódy spracovania. Práca je rozdelená do úvodu, troch číslovaných kapitol a záveru.

Z hľadiska štruktúry sa autor v prvých dvoch kapitolách venuje teoretickému a formálnemu fungovaniu systémov detekcie prienikov. Prvá kapitola ponúka štruktúrovaný úvod do zvolenej problematiky počítačovej bezpečnosti, systémov ochrany IDS, ich kategorizáciu a delenie z pohľadu rôznych perspektív. Obsiahlejšiu druhú kapitolu tvorí prehľad vybraných metód a algoritmov detekcie prienikov spolu s hodnotením ich efektivity pri detekcii hrozieb. Autor popisuje matematické, štatistické a pravdepodobnostné metódy používané na detekciu prienikov. Štruktúra a spracovanie je prehľadné, rozsah analyzovaných zdrojov je obsiahly, čo poukazuje na komplexnosť problematiky a množstvo oborov, ktoré sa bezpečnosti venujú. Je trochu na škodu, že analyzované sú zdroje skôr staršieho dáta, čo však autor odôvodňuje snahou poskytnúť prehľad „vybranej vzorky naprieč relevantným obdobiam existencie týchto technológií“.

Hlavnú časť práce s prezentáciou výsledkov autora tvorí tretia kapitola. V nej sa habilitant zameriava na riešenie metód systémov detekcie prienikov, zvýšenie výkonu IDS a efektivite v oblasti zberu a agregácie dát v sieťovom prostredí. 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 štyroch oblastí výskumu bezpečnosti a to:

- Oblasť 1: výskum v oblasti klasifikácie prienikov.
- Oblasť 2: riešenie výkonnosti a optimalizácia činnosti IDS systémov
- Oblasť 3: vývoj v oblasti monitoringu sietí
- Oblasť 4: ochrana cez honeypot systémy

Prvej oblasti sa venujú prvé dve publikácie. V nich sa autor a kolektív venujú oblasti klasifikácie anomálií, kde autor navrhol viacero riešení pre metódu samotnej detekcie pre HIDS systémy. Metódy využívajú klasifikácie pomocou samoorganizujúcich máp a čiastočne usporiadaných udalostí identifikovaných špecifickými znakmi, kde modelovanie prechodových stavov udalostí ako indikátor anomálií bolo riešené prostredníctvom Petriho sietí.

Druhej oblasti sa venujú nasledujúce tri publikácie od 3.3 po 3.5. Predmetom výskumu autora je distribuované spracovanie a optimalizáciu výkonu detekcie systému senzorov sieťových IDS nasadených v heterogénnom prostredí. Presun k distribuovaným systémom bol následkom výpočtovej náročnosti detekcie vo vysokorýchlostnom sieťovom prostredí. Riešením bola snaha o rozloženie výpočtovej zložitosti do viacerých agregačných a výpočtových rovín spolu so snahou o optimalizáciu vzorkovania analyzovaných dát využiteľných pre hybridnú detekciu. Návrh na základe výstupov z publikácií ponúkal zvýšenie výkony detekcií.

Tretej podoblasti sa venujú tri publikácie 3.6 až 3.8. V nich sa autor venuje oblasti monitoringu a zberu údajov v sieťovom prostredí opäť s bližším zameraním na objem a výkon. Dôraz je kladený na zefektívnenie metód zberu dát cez adaptabilné vzorkovanie sieťového toku či agregáciu nazbieraných hodnôt. Metódy sú zároveň využiteľné na sledovanie správania v sieti ako aj v systémoch detekcie prienikov na báze správania.

Posledná štvrtá oblasť je tvorená jedným karentovaným príspevkom zameraným na oblasť poznávania krokov útočníkov ako aj zabezpečenia sietí systémami lákadiel či pascí, tzv. honeypot-ov.

Predložený súbor prác vznikol ako súčasť viacročných výskumných aktivít autora v rámci riešenia výskumných úloh projektov VEGA (2) a APVV (2) a projektov rôznych operačných programov (4). Súbor prác predstavujú práce publikované v domácich karentovaných časopisoch (2), zahraničných recenzovaných zborníkoch (4), domácich časopisoch (2) a zborníkoch z domácich konferencií (1). Kladne hodnotím, že výskum vo vybraných oblastiach viedol k dvom karentovaným publikáciám z nedávneho obdobia. Práca je napísaná prehľadne, formálne aj obsahovo je vhodne členená. Písaná je zrozumiteľne, jednotlivé kapitoly na seba nadväzujú. Vybrané publikované práce autora deklarujú prínos v oblasti bezpečnosti a systémov detekcie prienikov. Z pohľadu posledných karentových výstupov hlavne v oblasti detekcie prienikov metódou lákadiel a návrhov metód adaptabilnej agregácie zbieraných údajov v sieťovom prostredí.

Vo vedeckej činnosti sa habilitant dlhodobo venuje problematike bezpečnosti sieťovej komunikácie ako aj súvisiacim doménam v oblasti informatiky. Tomu odpovedá aj publikačná činnosť autora, ktorá obsahuje 119 záznamov. Celkovo tak za oblasť VV 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 autor 15 rokov vedie cvičenia predmetov, ktoré súvisia s predmetom výskumu. Oceňujem jeho zapájanie do pedagogického procesu aj z pozície jeho terajšej profesie. Habilitant je autorom jednej VŠ učebnice a jedného skripta. Viedol 25 záverečných prác, bol zapojený do riešenia 2 KEGA projektov a 7 univerzitných projektov zameraných na oblasť vzdelávania. Jeho pedagogické aktivity považujem za primerané a prispievajúco k výchove študentov v odbore.

K téme predloženej habilitačnej práce mám nasledujúce otázky:

- V prípade technológie detekcie prienikov na princípe lákadiel, môže autor bližšie popísať výhody prístupu voči tradičným IDS?

- Ako autor vidí oblasť sieťovej bezpečnosti z hľadiska nasadenia systémov s prvkami umelej inteligencie a neurónových sieti?
- Ako vidí autor budúcnosť riešenia bezpečnosti v sieťovom prostredí, ktoré je vďaka nástupu Cloud systémov, IoT a podobných vecí mnohokrát veľmi rozľahlo rozprestreté bez centrálnych miest, kde je možné nasadiť Fw/IPS?
- Ako vidí autor možnosť technologickej a najmä procesnej implementácie bezpečnosti v tak „voľnom“ prostredí ako sú univerzity? Ako vidí stav a má názor na zabezpečenie slovenských univerzít?

Na základe celkového zhodnotenia predloženej práce, VV či pedagogických aktivít, ako aj naplnenia habilitačných kritérií konštatujem vysokú odbornú a pedagogickú úroveň habilitanta v predmetnej oblasti. Preto odporúčam habilitačnej komisii a Vedeckej rade Fakulty elektrotechniky a informatiky TU v Košiciach vymenovať Ing. Martina Chovanca, PhD. za
docenta
v odbore habilitačného konania: Informatika.

Predloženú habilitačnú prácu na základe predchádzajúceho hodnotenia

ODPORÚČAM prijať k obhajobe

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

Podpisom na tomto posudku zároveň súhlasím s licenčnými podmienkami obsiahnutými v licenčnej zmluve na použitie posudku záverečnej práce, ktorá je súčasťou tohto posudku.

Dátum: 20.05.2020 .....
podpis autora posudku