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: **prof. RNDr. Valerie Novitzká, PhD.**

Pracovisko oponenta: ***Katedra počítačov a informatiky***

KOMENTÁR OPONENTA HABILITAČNEJ PRÁCE
AKTUÁLNOSŤ ZVOLENEJ TÉMY HABILITAČNEJ PRÁCE:

Predložená habilitačná práca sa zaoberá bezpečnosťou sieťovej komunikácie a rieši niektoré aspekty a metódy existujúcich systémov, ktoré vykonávajú detekciu nežiaducich prienikov. Z hľadiska súčasného stavu v sieťovej komunikácii, ktorej intenzita a dôležitosť neustále rastie, pokladám tému práce za vysoko aktuálnu. Neželané a neodhalené prieniky môžu výrazne poškodiť prostredie, v ktorom sieťová komunikácia prebieha a zneužiť, prípadne zničiť dôležité a dôverné údaje, preto sú dosiahnuté výsledky prezentované v habilitačnej práci významným prínosom v tejto oblasti.

METÓDY SPRACOVANIA HABILITAČNEJ PRÁCE:

Štruktúru habilitačnej práce možno rozdeliť na dve časti.
Prvá časť práce definuje základné pojmy a existujúce metódy detekcie prienikov. V prvej kapitole autor definuje pojmy počítačovej bezpečnosti a klasifikuje systémy detekcie prienikov. Druhú kapitolu venuje podrobnej analýze niektorých metód používaných v systémoch detekcie, ktoré sú založené na základe zneužitia, anomálie, špecifikácií. Záverom kapitoly autor stručne charakterizuje hybridné metódy a metódy detekcie vo vysokorýchlostných sieťach.
Druhú časť práce tvorí kapitola 3, ktorá obsahuje 9 prác publikovaných v domácich a medzinárodných časopisoch a prezentovaných na medzinárodných vedeckých konferenciách.

DOSIAHNUTÉ VÝSLEDKY HABILITAČNEJ PRÁCE A NOVÉ POZNATKY:

Výsledky svojej práce a dosiahnuté výsledky autor dokumentuje svojimi publikáciami v kapitole 3, ktoré publikoval ako člen výskumného tímu. Autor usporiadal publikácie, v ktorých je spoluautorom, podľa vývoja a orientácie svojho výskumu od roku 2006 až po rok 2019.
Najdôležitejšie dosiahnuté výsledky autora sú publikované v dvoch domácich karentovaných časopisoch.
Článok v kapitole 3.8 je venovaný problematike monitorovania sieťovej prevádzky so zameraním na spracovanie rozsiahlych dát. Autori navrhli nový a zaujímavý prístup, ktorý adaptívne agreguje záznamy toku a umožňuje automatické prispôsobenie svojej práce podľa skutočného zaťaženia siete a potrieb monitorovania.
V článku v kapitole 3.9 je návrh a architektúra sofistikovaného hybridného lákadla, ktoré je schopné presmerovať rušivý prenos a generovať varovania. Rozšírením pôvodnej architektúry hybridného lákadla autori navrhli a experimentálne overili nový systém, ktorý už má črty reaktívneho systému.
Obidva články majú vysokú kvalitu a podľa značného počtu ohlasov na ne konštatujem, že predstavujú dôležitý prínos v skúmanej oblasti informatiky.

PRÍNOS PRE ĎALŠÍ ROZVOJ VEDY A TECHNIKY (UMENIA):

Dosiahnuté a publikované výsledky výskumnej práce habilitanta spolu s množstvom citácií na jednotlivé práce potvrdzujú ich dôležitosť a potvrdzujú významný prínos autora k rozvoju disciplíny bezpečnosti sieťovej komunikácie.

PRIPOMIENKY A POZNÁMKY K HABILITAČNEJ PRÁCI:

Práca je napísaná precízne, bez typografických chýb.
K čitateľnosti práce by prispelo, keby autor použil preprinty všetkých priložených publikácií s informáciou kde boli publikované, nielen ich texty.

OTÁZKY K RIEŠENEJ PROBLEMATIKE:

1. Autor v druhej časti práce prezentuje dva články kategórie B, podľa knižničného poriadku odborné články. Aký bol dôvod zaradiť ich do habilitačnej práce medzi najdôležitejšie výskumné výsledky autora?
2. Výskumná činnosť autora pokrýva široké spektrum z oblasti bezpečnosti sieťových komunikácií. Akým smerom predpokladá svoj ďalší výskum?

SPLNENIE SLEDOVANÝCH CIEĽOV HABILITAČNEJ PRÁCE:

Ciele, ktoré si habilitant stanovil, boli v tejto práci dosiahnuté. Práca poskytuje prierez jeho kontinuálnej výskumnej práce v oblasti počítačových sietí a ich bezpečnosti a je predpokladom jeho ďalšieho vedeckého I pedagogického rastu.

CELKOVÉ ZHODNOTENIE HABILITAČNEJ A ZÁVER:

Habilitant touto prácou preukázal svoju erudovanosť a vedeckú spôsobilosť v oblasti bezpečnosti počítačovej komunikácie. Splnil všetky kritériá požadované pre habilitačné konanie, preukázal hlboké vedomosti a tvorivosť pri svojej výskumnej práci a je perspektívnym pracovníkom v oblasti bezpečnosti sieťových komunikácií.

Jeho publikačné výsledky, zhodnotenie jeho pedagogickej práce v danej oblasti a účasť na riešení výskumných projektov ma oprávňujú odporučiť habilitačnej komisii prijať túto prácu a po úspešnej obhajobe udeliť Ing. Martinovi Chovancovi, PhD. vedecko-pedagogický titul " docent" v odbore 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: 04.05.2020 .....

podpis autora posudku