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. Ing. Pavel Čičák, PhD.**

Pracovisko oponenta: ***FIIT STU v Bratislave***

KOMENTÁR OPONENTA HABILITAČNEJ PRÁCE
AKTUÁLNOSŤ ZVOLENEJ TÉMY HABILITAČNEJ PRÁCE:

Problematika počítačových sietí prerástla v súčasnosti do novej dimenzie. Všetko začalo prepájaním počítačov. Zatiaľ čo v nedávnej minulosti pribudlo prepojenie vecí, v súčasnosti je predmetom prepájania „všetko“. Preto téma habilitačnej práce „detekcia prienikov v oblasti bezpečnosti sieťovej komunikácie“ je vysoko aktuálna a predpokladá sa, že v blízkej budúcnosti sa bude aj veľmi dynamicky rozvíjať. Predložená práca je zameraná na vyhodnocovanie vybraných metód detekcie prienikov do priestoru počítačových sietí.

METÓDY SPRACOVANIA HABILITAČNEJ PRÁCE:

Metodika, systematičnosť a spôsob spracovania témy v práci svedčí o vysokej pedagogickej a odbornej erudovanosti habilitanta v sledovanej problematike.
Práca je koncipovaná ako komentovaný súbor vybraných publikácií autora a kolektívu tematicky orientovaných na detekcie prienikov v oblasti bezpečnosti sieťovej komunikácie. Je formálne rozdelená do troch hlavných kapitol a osemnástich podkapitol, vrátane úvodu, vybraných príspevkov autora k uvedenej téme, zoznamu výskumno-pedagogických projektov autora, ako aj publikačnej činnosti autora. Predložená práca obsahuje 178 strán textu a autor použil 146 literárnych prameňov. Habilitant približuje problematiku detekcie prienikov v oblasti sieťových komunikácií vo všeobecnosti. Rozoberá prístupy, formy, metódy a naznačuje aj teoretické princípy vrátane formálneho aparátu.

DOSIAHNUTÉ VÝSLEDKY HABILITAČNEJ PRÁCE A NOVÉ POZNATKY:

Samotná časť práce, ktorá sa zaoberá vedecko-výskumnými výsledkami je koncipovaná ako komentovaný súbor vybraných publikácií autora a kolektívu tematicky orientovaných na oblasť problematiky detekcie prienikov v oblasti sieťových komunikácií vo všeobecnosti. Habilitant sa predmetnej oblasti venuje bezmála 15 rokov. Za toto obdobie sa technologické prostredie sieťových komunikácií výrazne vyvíjalo, čo sa prejavilo nielen v obsahu, ale aj témach jeho publikácií. Keďže z tohto dôvodu nie je jednoduché obsiahnuť všetky publikácie a prístupy, autor zo 46 publikácií zvolil prehľad systémov a metód vo forme vybranej vzorky naprieč relevantným obdobiam existencie a vývoja technologického prostredia sieťovej komunikácie.
Predmetné výstupy sú zamerané na oblasť bezpečnosti, kde sa autor primárne venuje systémom detekcie prienikov a ich efektivite v sieťovom prostredí.
Z hľadiska postupnosti výskumu, aj osobnej profilácie autora, je možne rozdeliť problematiku výskumu na tri oblasti:

- oblasť klasifikácie, t.j. jadra detekcie, kde v rámci vybraných metód habilitant spolu s kolektívom navrhli viacero pôvodných riešení na samotnú detekciu,
- oblasť optimalizácie systému narušenia bezpečnosti z hľadiska zberu a spracovania údajov aplikáciou systému multi-senzorov vrátane výkonnostných aspektov, čiže schopnosť detekcie vo vysokorýchlostných sieťach aplikáciou metód distribuovaného a vysokovýkonného spracovania,
- oblasť vývoja protokolov a algoritmov pre monitoring sieťovej prevádzky, kde sa autor spolu s kolektívom zameral na návrh optimálneho protokolu pre monitoring sieťovej prevádzky metódami vzorkovania s cieľom zvýšenia výkonu a efektivity prenosu získavaných údajov pre systém detekcie priamo zo sieťových zariadení.

Okrem časopiseckých a konferenčných výstupov výskum vo vybraných oblastiach viedol k dvom karentovaným publikáciam v oblasti bezpečnosti počítačových sieti a systémov. Ide o systém detekcie prienikov s využitím hybridných lákadiel a optimalizáciu monitorovacích protokolov so zameraním na zber údajov a charakteristík v komunikačných sieťach.

PRÍNOS PRE ĎALŠÍ ROZVOJ VEDY A TECHNIKY (UMENIA):

Predloženú habilitačnú prácu je možné vnímať v dvoch rovinách. Jedna časť je vlastne monografická resp. monotematická, ktorá preukazuje vysokú erudovanosť habilitanta nielen po odbornej, ale najmä pedagogickej stránke. Opisuje a uvádza analýzu a vlastné pohľady na oblasť vedy, ktorej sa dlhodobo venuje. Jedná sa o bezpečnostné aspekty, formy, metódy a teoretické prístupy k detekcii prienikov v prostredí sieťovej komunikácie vo všeobecnosti. Čo je dôležité formuluje aj ďalšie možnosti, trendy a predpokladaný vývoj metód detekcie prienikov najmä s ohľadom na stále sa rozširujúce prepájanie „všetkého“ (IoE).
Druhá časť práce uvádza doteraz skúmané oblasti vrátane konkrétnych výstupov a to:

- detekciu zneužitia
  - vzory útokov

o signatúry
• detekcie anomalii
o na báze učenia
o hybridné systémy
a uvádza ďalšie smery možného výskumu.

PRIPOMIENKY A POZNÁMKY K HABILITAČNEJ PRÁCI:
Zásadné pripomienky k habilitačnej práci nemám. Práca je po formálnej stránke spracovaná na veľmi dobrej úrovni. V práci nie je v niekoľkých prípadoch uvedený odkaz na použitú literatúru a taktiež nie sú vo všetkých prípadoch dôsledne špecifikované zdroje zrejme použitých obrázkov resp. matematických vzťahov. Každá kapitola je dopĺňaná grafickými znázorneniami a obrázkami. Práca je písaná jasne a zrozumiteľne, je systematicky spracovaná a na úrovni zodpovedajúcej kritériám pre priznanie vedecko-pedagogického titulu docent.

PRIPOMIENKY A POZNÁMKY K HABILITAČNEJ PRÁCI:

Zásadné pripomienky k habilitačnej práci nemám. Práca je po formálnej stránke spracovaná na veľmi dobrej úrovni. V práci nie je v niekoľkých prípadoch uvedený odkaz na použitú literatúru a taktiež nie sú vo všetkých prípadoch dôsledne špecifikované zdroje zrejme použitých obrázkov resp. matematických vzťahov. Každá kapitola je dopĺňaná grafickými znázorneniami a obrázkami. Práca je písaná jasne a zrozumiteľne, je systematicky spracovaná a na úrovni zodpovedajúcej kritériám pre priznanie vedecko-pedagogického titulu docent.

OTÁZKY K RIEŠENEJ PROBLEMATIKE:

K práci mám nasledujúce otázky:
1. Autor v rámci súboru publikácií v podoblastiach 1 a 2 uvádza rôzne metódy a variácie systémov detekcie prienikov, je možné z jeho strany porovnať uvedené návrhy z hľadiska efektivity a presnosti detekcie?
2. Súbor publikácií v podoblasti 3(kapitoly 3.6 až 3.8) smerujú k návrhu adaptívnej agregácii záznamov sieťových tokov. V akých systémoch IDS je predpokladáte využitie týchto údajov, aké výhody resp. nevýhody poskytuje tento prístup v oblasti IDS?
3. Autor sa v kapitole 3.9. habilitačnej práce zameriava na výskum v oblasti lákadiel, pričom uvádza vybrané výhody tejto architektúry voči systémom IDS. Bolo by možné prieniky identifikované týmto systémom využiť aj v oblasti tradičných IDS, ak áno, akým spôsobom?
4. Systémy detekcie prienikov sú aktuálne súčasťou viacerých komerčných riešení v oblasti zabezpečenia informačno-komunikačných technológií , aké metódy a architektúry na tento účel využívajú v porovnaní s prístupmi autora?

SPLNENIE SLEDOVANÝCH CIEĽOV HABILITAČNEJ PRÁCE:

Pri posudzovaní plnenia Kritérií na habilitácie docentov FEI TU konštatujem, že habilitant plní platné kritériá, prejavil schopnosť jasného a zrozumiteľného interpretovania problematiky a vhodne využil matematický aparát pre opis skúmaných javov.
Vo vedeckej činnosti sa habilitant dlhodobo venuje oblasti počítačových sietí, mechanizmom pre detekciu prienikov v oblasti bezpečnosti sieťovej komunikácie ako aj viacerým aplikačným doménam do ktorých poznatky prenáša. Nezanedbateľná je účasť habilitanta na riešení a vedení viacerých grantových projektov.
Z habilitačnej práce a priložených dokladov vyplýva, že Ing. Martin Chovanec, PhD. je pedagogicky a vedecky skúsenou osobnosťou so schopnosťami prenášať najnovšie teoretické poznatky a praktické skúsenosti do pedagogickej a vedeckovýskumnej činnosti.

CELKOVÉ ZHODNOTENIE HABILITAČNEJ A ZÁVER:

Na základe celkového zhodnotenia habilitačnej práce a posúdením faktov a stanovísk z priložených dokladov (Profesijný životopis, Prehľad pedagogickej činnosti a výsledkov dosiahnutých vo výchovno-vzdelávacej činnosti, Prehľad vedecko-výskumnej činnosti a výsledkov dosiahnutých v tejto oblasti, Zoznam pôvodných publikovaných vedeckých a odborných prác, učebníc, učebných textov, Plnenie kritérií FEI TU v Košiciach pre habilitačné konanie)
konštatujem,
že habilitačná práca, ako aj vedecká spôsobilosť Ing. Martina Chovanca, PhD. zodpovedajú požiadavkám habilitácie a
odporúčam,
aby v prípade úspešnej habilitácie bol

Ing. Martin Chovanec, PhD.
vymenovaný 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: 06.05.2020 .....
podpis autora posudku