FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Vedoucí práce:	Ing. Tomáš Čejka, Ph.D.
Student:	Tomáš Klatovský
Název práce:	Detekce síťového provozu aplikace TeamViewer
Obor / specializace:	Bezpečnost a informační technologie
Vytvořeno dne:	7. června 2021

Hodnotící kritéria

1. Splnění zadání

- ▸ [1] **zadání splněno**
  [2] zadání splněno s menšími výhradami
  [3] zadání splněno s většími výhradami
  [4] zadání nesplněno

Práce se zabývá identifikací a klasifikací komunikace aplikace TeamViewer pro vzdálenou správu. Tento provoz v určitých situacích může znamenat bezpečnostní hrozbu, obzvláště pokud dojde ke spuštění této komunikace bez vědomí uživatele nebo správce infrastruktury. Tato práce navazuje na existující publikované práce, které student důkladně prozkoumal, a na rozdíl od těchto prací je vytvořené řešení této bakalářské práce založené na analýze rozšířených IP toků, které lze snáze získat i z vysokorychlostních linek, a dosahuje dostatečně dobrých výsledků, což je v praxi mnohem použitelnější než stávající řešení.

2. Písemná část práce 89 / 100 (B)

Práce má dobrou strukturu, ale některé formulace jsou trochu obtížněji srozumitelné. Práce obsahuje drobné typografické nedostatky. Celkově je však text práce kvalitní, v anglickém jazyce, což přispěje k rozšíření výsledků v rámci vědecko-výzkumné komunity.

3. Nepísemná část, přílohy 95 / 100 (A)

Výstupem práce jsou datové sady vytvořené jednak manuálně a následně i s využitím reálného anotovaného síťového provozu. Dalším významným výstupem bakalářské práce je sada experimentů, z nichž vychází prototyp klasifikace síťového provozu založený na metodách strojového učení. Na základě důkladných testů se zdají výsledky úspěšné. Vytvořený prototyp proto může sloužit k realizaci optimalizované produkční verze klasifikačního modulu.

4. Hodnocení výsledků, jejich využitelnost 95 /100 (A)

Klasifikace síťového provozu bez narušení soukromí (skrze dešifrování nebo analýzu obsahu komunikace) může pomoci zvýšit situační povědomí správců a bezpečnostních analytiků. Proto je navržené a vytvořené řešení založené na rozšířených IP tocích zajímavé a využitelné v praxi. Výsledky práce mají, dle mého názoru, publikační potenciál.

5. Aktivita studenta

▸ [1] **výborná aktivita**
[2] velmi dobrá aktivita
[3] průměrná aktivita
[4] slabší, ale ještě dostatečná aktivita
[5] nedostatečná aktivita

Student se aktivně zapojil do činností týmu Laboratoře monitorování síťového provozu, v rámci kterého řešil zadání této bakalářské práce. Účastnil se pravidelných schůzí týmu, na které byl vždy skvěle připraven. Student byl aktivní po celou dobu práce na tomto zadání a díky tomu se podařilo dosáhnout skvělých výsledků.

6. Samostatnost studenta

▸ [1] **výborná samostatnost**
[2] velmi dobrá samostatnost
[3] průměrná samostatnost
[4] slabší, ale ještě dostatečná samostatnost
[5] nedostatečná samostatnost

Student pracoval samostatně a zadané úkoly svědomitě plnil.

Celkové hodnocení 92 /100 (A)

Odevzdaná bakalářská práce je kvalitní a může být základem pro budoucí vědecko-výzkumnou publikaci. Výsledky jsou uplatnitelné v praxi především pro detekci podezřelé komunikace vzdálené správy, čímž se správcům a bezpečnostním týmům zlepší přehled nad síťovým provozem. Text práce by se sice ještě dal lehce zlepšit, ale přesto tato práce celkově patří k velmi zdařilým.

Instrukce

Splnění zadání

Posuďte, zda předložená ZP dostatečně a v souladu se zadáním obsahově vymezuje cíle, správně je formuluje a v dostatečné kvalitě naplňuje. V komentáři uveďte body zadání, které nebyly splněny, posuďte závažnost, dopady a případně i příčiny jednotlivých nedostatků. Pokud zadání svou náročností vybočuje ze standardů pro daný typ práce nebo student případně vypracoval ZP nad rámec zadání, popište, jak se to projevilo na požadované kvalitě splnění zadání a jakým způsobem toto ovlivnilo výsledné hodnocení.

Písemná část práce

Zhodnoťte přiměřenost rozsahu předložené ZP vzhledem k obsahu, tj. zda všechny části ZP jsou informačně bohaté a ZP neobsahuje zbytečné části. Dále posuďte, zda předložená ZP je po věcné stránce v pořádku, případně vyskytují-li se v práci věcné chyby nebo nepřesnosti.

Zhodnoťte dále logickou strukturu ZP, návaznosti jednotlivých kapitol a pochopitelnost textu pro čtenáře. Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 26/2017, článek 3.

Posuďte, zda student využil a správně citoval relevantní zdroje. Ověřte, zda jsou všechny převzaté prvky řádně odlišeny od vlastních výsledků, zda nedošlo k porušení citační etiky a zda jsou bibliografické citace úplné a v souladu s citačními zvyklostmi a normami. Zhodnoťte, zda převzatý software a jiná autorská díla, byly v ZP použity v souladu s licenčními podmínkami.

Nepísemná část, přílohy

Dle charakteru práce se případně vyjádřete k nepísemné části ZP. Například: SW dílo – kvalita vytvořeného programu a vhodnost a přiměřenost technologií, které byly využité od vývoje až po nasazení. HW – funkční vzorek – použité technologie a nástroje, Výzkumná a experimentální práce – opakovatelnost experimentů.

Hodnocení výsledků, jejich využitelnost

Dle charakteru práce zhodnoťte možnosti nasazení výsledků práce v praxi nebo uveďte, zda výsledky ZP rozšiřují již publikované známé výsledky nebo přinášející zcela nové poznatky.

Aktivita studenta

V souvislosti s průběhem a výsledkem práce posuďte, zda byl student během řešení aktivní, zda dodržoval dohodnuté termíny, jestli své řešení průběžně konzultoval a zda byl na konzultace dostatečně připraven.

Samostatnost studenta

V souvislosti s průběhem a výsledkem práce posuďte schopnost studenta samostatné tvůrčí práce.

Celkové hodnocení

Shrňte stránky ZP, které nejvíce ovlivnily Vaše celkové hodnocení. Celkové hodnocení nemusí být aritmetickým průměrem či jinou hodnotou vypočtenou z hodnocení v předchozích jednotlivých kritériích. Obecně platí, že bezvadně splněné zadání je hodnoceno klasifikačním stupněm A.