FAKULTA
INFORMAČNÍCH
TECHNOLOGIÍ
ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Vedoucí práce:	Ing. Tomáš Čejka, Ph.D.
Student:	Lukáš Jančička
Název práce:	Klasifikace komunikace uvnitř Tor spojení
Obor / specializace:	Teoretická informatika
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 netriviálním tématem analýzy a klasifikace šifrovaného provozu anonymizační služby Tor. Během práce proběhlo důkladné prostudování charakteristik tohoto komunikačního protokolu na úrovni síťových paketů a toků s cílem připravit dostatečně reprezentativní datové sady pro návrh klasifikačního modulu. Výsledkem je detailní rešerše a z praktické části i navržený a otestovaný klasifikátor pro rozpoznání Tor komunikace a tříd komunikace přes Tor. Zadání se tímto podařilo úspěšně splnit.

2. Písemná část práce 95 / 100 (A)

Práce je dobře strukturovaná, a obsahuje pouze zanedbatelné typografické nedostatky. Celkově je práce na velice vysoké úrovni kvality, svou výzkumnou povahou a rozsahem prací se spíše blíží k diplomové práci. Navíc je text práce vytvořen v anglickém jazyce, což přispěje k rozšíření výsledků v rámci vědecko-výzkumné komunity. Jazykově se práce zdá být v pořádku.

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

Výstupem práce je sada experimentů, v rámci kterých proběhla analýza zachyceného síťového provozu aplikace Tor. Student navrhl a vytvořil klasifikační algoritmus založený na známých modelech strojového učení a tento algoritmus natrénoval a odladil tak, aby dosáhl co největší přesnosti klasifikace. Na základě důkladných testů se zdají výsledky úspěšné. Vytvořený prototyp může sloužit k realizaci optimalizované produkční verze klasifikačního modulu.

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

Výsledky této práce je možné hodnotit ze dvou různých pohledů. Služba Tor by měla, dle očekávání uživatelů, zajišťovat anonymitu aktivit na internetu. Tato bakalářská práce však ukazuje, že je provoz Tor možné identifikovat na základě statistik rozšířených IP toků a navíc je možné odhadovat i třídu aktivit. Z druhého pohledu se jedná o službu často zneužívanou ke kriminální činnosti, a proto klasifikace síťového provozu bez narušení soukromí (skrze dešifrování nebo analýzu obsahu komunikace) může pomoci zvýšit situační povědomí správců a bezpečnostních analytiků. V každém případě jsou výsledky této práce zajímavé a užitečné v praxi. Navíc 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 stal důležitou součástí týmu Laboratoře monitorování síťového provozu, 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 byl maximálně samostatný a veškeré zadané úkoly související se směřováním této závěrečné práce svědomitě plnil. Nad rámec tohoto zadání se student iniciativně věnoval souvisejícímu vyhodnocování datových sad, čímž přispěl i ostatním členům týmu Laboratoře monitorování síťového provozu.

Celkové hodnocení 100 /100 (A)

Odevzdaná bakalářská práce je velice kvalitní, výsledky mají publikační potenciál a uplatnění v praxi pro zvýšení přehledu nad síťovým provozem kvůli bezpečnosti infrastruktury.

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.