FAKULTA
INFORMAČNÍCH
TECHNOLOGIÍ
ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Vedoucí práce:	Ing. Karel Hynek
Student:	Bc. Dmitrii Vekshin
Název práce:	Detekce zneužívání DNS over HTTPS
Obor / specializace:	Počítačová bezpečnost
Vytvořeno dne:	6. února 2023

Hodnotící kritéria

1. Splnění zadání

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

V rámci závěrečné práce mělo být prozkoumáno state-of-the-art šifrovaného DNS, konkrétně DNS over HTTPS. Student se této části poctivě věnoval a vytvořil informačně bohaté shrnutí. Bohužel druhá část zadání a to vytvoření prototypu síťového detektoru tunelovaného provozu skrz DNS over HTTPS (DoH) protokol nebyla splněna, protože ji student nestihl. Chybí tedy popis návrhu a vyhodnocování algoritmu, popis implementace prototypu a jeho testování.

2. Písemná část práce

60 / 100 (D)

Písemná část je psána v angličtině a bohužel obsahuje velké množství překlepů, typografických a gramatických chyb a často nesrozumitelných vět či dokonce nesrozumitelných názvů sekcí (Např.: sekce Demand on the protocol). Členění písemné části je většinou logické, zaznamenal jsem jen drobné nedostatky u popisu datové sady, kde bych pořadí sekcí přeuspořádal. Obsahově jsou první tři kapitoly bohaté, čtvrtá kapitola je ale zjevně dokončovaná narychlo.

V textu jsem našel několik faktických chyb, například v Tabulce 1.2 je napsáno, že DNS over QUIC nepoužívá fixní port, to ale není pravda. V citovaném RFC9250 je přesně definovaný port 853/UDP. Dále přisuzované autorství společnosti Google protokolů JSON DNS a DNS over QUIC také určitě není pravdivé, protože Google nefiguruje jako autor ani jednoho RFC. Dále se v textu nedefinují zkratky před jejich prvním použitím, což může být občas zmatečné. DoT může být DNS over TLS, DNS over TOR, nebo DNS over Telegram. Bohužel ani seznam zkratek není úplný.

Práce cituje celkem 85 různých zdrojů, což považuji za nadprůměrné číslo. Je vidět, že si student dal s rešerší opravdu velkou práci. Bohužel některé citace jsou ale neúplné a citované webové stránky nemají url---např citace 83.

3. Nepísemná část, přílohy 30 /100 (F)

Nepísemná část obsahuje skripty pro generování datové sady a jupyter notebook s trénováním modelu. Jupyter notebook je sice anotován pomocí jazyka markdown, rozhodně se však ale nedosahuje kvalit kladených na finální výstupy závěrečných prací. Závěrečná práce navíc výsledky klasifikace nijak nekomentuje a proto je těžké v nich najít relevantní informace. Nepísemné přílohy neobsahují prototyp schopný zpracovávat reálný síťový provoz, který byl uveden v zadání práce.

4. Hodnocení výsledků, jejich využitelnost 40 /100 (F)

Obsáhlé shrnutí současného vědění o protokolu DNS over HTTPS mi přijde velice užitečné. Rovněž skripty pro vytváření datové sady a prvotní experimenty s klasifikací mi přijdou relativně dobré, ale v současném stavu je jejich využitelnost značně omezená. Chybějící dokumentace, komentáře a nečitelnost kódu ale tvoří neúplný výsledek, na který se bude jen těžko navazovat.

5. Aktivita studenta

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

Student začal být aktivní až v pozdějších fázích, z čehož vyplývá že práci bohužel nestihl.

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.

Celkové hodnocení 40 /100 (F)

Student věnoval velké úsilí studiu rešerše a tvorbě datové sady a to je i v textu práce vidět. Bohužel nestihl datovou sadu využít k návrhu a implementaci prototypu detektoru. Spěch je bohužel vidět i v samotném textu, který obsahuje velké množství překlepů a typografických chyb. Vzhledem k nesplnění podstatné části zadání nemohu hodnotit práci jinak, než stupněm F.

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. 52/2021, 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.