FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Student:	Bc. Samuel Hanák
Oponent práce:	Ing. Tomáš Čejka, Ph.D.
Název práce:	Fingerprinting prohlížeče - techniky a obrana
Obor:	Počítačová bezpečnost

Datum vytvoření: 4. 6. 2020

Hodnotící kritérium:	*Způsob hodnocení – následující škálou 1 až 4:*
1. Splnění zadání	***1=zadání splněno,*** *2=zadání splněno s menšími výhradami,* *3=zadání splněno s většími výhradami,* *4=zadání nesplněno*

Popis kritéria:
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.

Komentář:
Práce se zabývá technikami identifikace webových prohlížečů (tzv. fingerprinting) a obranou proti nim. Text práce shrnuje aktuální poznatky v této oblasti a popisuje detailněji jak techniky identifikace tak i obrany. Praktická část práce se zabývá rozšířením HTTP proxy Privoxy o několik vybraných metod obrany. Vzhledem k tomu, že zadání neobsahuje žádné konkrétní metody, které bylo potřeba implementovat, považuji zadání za splněné s komentáři v dalších sekcích.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
2. Písemná část práce	*95 (A)*

Popis kritéria:
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.

Komentář:
Text závěrečné práce je kvalitní, dobře členěný a srozumitelný. V textu jsem našel pouze drobné typografické nedostatky. Text je informačně bohatý a popsané metody jsou doplněny názornými ukázkami, které usnadňují pochopení - teoreticky lze práci využít pro výukové účely.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
3. Nepísemná část, přílohy	*80 (B)*

Popis kritéria:
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

Komentář:
Nepísemná část práce spočívá v rozšíření funkcionality Privoxy o metody obrany proti identifikaci prohlížeče/uživatele. Jedná se konkrétně o rozšíření možností filtračních a přepisovacích funkcí Privoxy. Písemná část práce diskutuje často používané nástroje pro testování fingerprinting technik, avšak později v textu v Sekci 5.2 autor uvádí, že tyto nástroje nebylo možné použít. Proto se zdá, že volba implementovaných obranných technik proběhla s ohledem na co nejjednodušší realizaci místo mnohem důležitějšího dopadu na účinnost obrany, což je u diplomové práce škoda. Navíc tato volba bohužel nebyla podložena měřením, které by ukázalo, že obranné metody, na které se zaměřují nejpoužívanější testovací nástroje, nejsou potřeba v praxi.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*

4. Hodnocení výsledků, jejich využitelnost

89 (B)

Popis kritéria:
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.

Komentář:

Dle celkového dojmu jsem dospěl k názoru, že hlavní přínos celé práce je především v teoretické písemné části práce, která je dobře a přehledně zpracovaná. Vyvinuté úpravy nástroje Privoxy jsou funkční a použitelné. Je zřejmé, že bez důkladné analýzy v písemné části by vylepšení nebyla realizovatelná. Filtrace a modifikace obsahu komunikace se zdá být na základě této analýzy již jednoduchou úlohou. Z pohledu využitelnosti se mi zdá, že se autor mohl pokusit alespoň o jednoduchý prototyp složitější obrany proti technikám založených na interakci s prohlížečem pomocí JavaScript skriptů. Tím pádem by bylo nejspíš možné provést alespoň základní vyhodnocení pomocí "nejpoužívanějších" testovacích nástrojů (viz otázky k obhajobě).

Hodnotící kritérium: *Způsob hodnocení – nehodnotí se*

5. Otázky k obhajobě

Popis kritéria:
Uveďte případné dotazy, které by měl student zodpovědět při obhajobě ZP před komisí (body oddělte odrážkami).

Otázky:

1) Dokážete odhadnout, jak moc se pomocí všech implementovaných metod obrany sníží pravděpodobnost úspěšné identifikace prohlížeče/uživatele?
2) Co by obnášela realizace obranných metody, které by byly testovatelné zmíněnými nástroji AmIUnique a Panopticlick?

Hodnotící kritérium: *Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*

6. Celkové hodnocení

89 (B)

Popis kritéria:
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.

Text hodnocení:

Tato práce prezentuje průzkum aktuálního stavu v oblasti technik identifikace prohlížečů, jednotlivé techniky podrobně a srozumitelně vysvětluje a k tomu diskutuje možné způsoby obrany. Písemnou část vnímám jako hlavní přínos celé práce, přestože i vyvinuté úpravy nástroje Privoxy jsou funkční a jejich účinek je prezentovatelný. V práci mi chybí vyhodnocení celkového vlivu implementovaných obranných technik na účinnost identifikace. Jinými slovy, jsou implementované metody dostatečné proti fingerprinting metodám?

Podpis oponenta práce: