FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Vedoucí práce:	Ing. Karel Hynek, Ph.D.
Student:	Matyáš Lhota
Název práce:	Rozšíření systému Zeek o unirec výstup
Obor / specializace:	Informační bezpečnost 2021
Vytvořeno dne:	31. května 2024

Hodnotící kritéria

1. Splnění zadání

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

Zadání bylo splněno v celém rozsahu. Navíc se v průběhu řešení diplomové práce ukázalo, že je i výrazně náročnější než bylo původně zamýšleno. Student si s tím ovšem velice dobře poradil.

2. Písemná část práce 95 /100 (A)

Rozsah práce (50 stran) převyšuje standardní délku bakalářské práce. Tento nadstandardní rozsah byl vyplněn informačně bohatými kapitolami, které jsou logicky členěné. Po věcné stránce jsem v práci nenarazil na žádnou chybu či nepřesnost. Vzhledem k implementačnímu zaměření práce považuji i počet referencí za dostatečný. Kromě drobných typografických či jazykových chyb (chybějící či přebývající členy a čárky) nemám k textu práce výhrad.

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

Hlavním obsahem nepísemné části jsou dva Zeek pluginy realizující export informací do systému NEMEA. První plugin je napsaný v jazyce C++ a byl implementován pro využití systému Zeek ve výkonnostně náročných nasazeních. I přes relativně složité API systému Zeek jsou C++ zdrojové kódy čitelné a neměl jsem problém s jejich porozuměním. Druhý plugin, napsaný pomocí skriptovacího jazyka Zeek, což je doporučovaná varianta vývoje nových pluginů. Implementace pluginu pomocí skriptovacího jazyka je srozumitelná a velice dobře čitelná. Celkově považuji nepísemnou část práce jako velice kvalitní.

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

Vytvořené pluginy jsou využitelné komunitou zabývající se síťovou bezpečnostní. Systém Zeek patří mezi nejoblíbenější nástroje pro monitorování síťového provozu a detekci síťových hrozeb. Vytvořené pluginy zajistí interoperabilitu systémů Zeek a NEMEA a zpřístupní tak nástroje systému NEMEA většímu množství uživatelů.

5. Aktivita studenta

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

Student chodil na domluvená setkání vždy včas a připraven.

6. Samostatnost studenta

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

Samostatnost byla vynikající. Student řešil problémy vlastní iniciativou, občas dokonce i s vývojáři samotného systému Zeek.

Celkové hodnocení 95 /100 (A)

V rámci práce došlo k důkladnému nastudování systému Zeek, jeho dokumentace a možností vývoje pluginu. C++ API systému Zeek se ovšem ukázalo jako výrazně složitější a málo dokumentované. Student z vlastní iniciativy proto vyrazil na vývojářskou konferenci FOSDEM, kde došlo ke schůzkám a navázání kontaktů s vývojáři Systému Zeek, kteří mu následně poskytovali cenné rady v průběhu vývoje. Veškeré překážky, problémy vývoje a jejich řešení jsou popsané v textu práce, která dokumentuje návrhová rozhodnutí a poskytuje výsledky z výkonnostních měření vyvinutých pluginů. Z výše uvedených důvodů považuji práci jako velice kvalitní a student na ní odvedl velké množství práce. Proto práci doporučuji k obhajobě a hodnotím stupněm A.

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.