Hodnocení vedoucího závěrečné práce

České vysoké učení technické v Praze **Fakulta informačních technologií**

Student: Richard Molnár
Vedoucí práce: Ing. Filip Štěpánek
Název práce: Pseudo-Random Numbers Prediction
Obor: Softwarové inženýrství

Datum vytvoření: 13. 6. 2017

Hodnotící kritérium:	*Způsob hodnocení - následující škálou 1 až 5:*
1. Náročnost a další komentář k zadání	***1=mimořádně náročné zadání,*** *2=náročnější zadání,* *3=průměrně náročné zadání,* *4=lehčí, ale ještě dostatečně náročné zadání,* *5=nedostatečně náročné zadání*

Popis kritéria:
Podrobněji charakterizujte diplomovou (bakalářskou) práci a její případné návaznosti na předchozí nebo běžící projekty. Dále posuďte, čím je zadání této ZP náročné. (U obtížnější ZP lze dále tolerovat některé nedostatky, které by u ZP standardní obtížnosti tolerovány nebyly; a naopak u jednoduché ZP mohou být zjištěné nedostatky hodnoceny přísněji.)

Komentář:
K úspěšné realizaci bylo potřeba nastudování problematiky PRNG (pseudo-náhodných číselných generátorů), která se vyučuje až v magisterském studiu. Dále byla potřeba důkladná analýza zdrojových kódů algoritmů užívaných pro generování pseudo-náhodných čísel v PHP a analýza procesu generování tzv. "seed" operačním systémem stroje, na kterém je nasazen webserver. Tyto problémy bylo třeba vyřešit k nalezení správného postupu, kterým by bylo možné zneužít slabiny ve stávajících implementacích generátorů pseudo-náhodných čísel.

Z těchto důvodu hodnotím zadání jako mimořádně náročné.

Hodnotící kritérium:	*Způsob hodnocení - následující škálou 1 až 4:*
2. 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 splňuje zadání. V komentáři uveďte body zadání, které nebyly zcela splněny, případně rozšíření ZP oproti původnímu zadání. Nebylo-li zadání zcela splněno, pokuste se posoudit závažnost, dopady a případně i příčiny jednotlivých nedostatků.

Komentář:
Zadání bylo splněno. Výstupem je funkční aplikace pro příkazovou řádku, která je schopná nalézt tzv. seed pseudo-náhodného generátoru v PHP. Aplikace je určena pro bezpečnostní specialisty, kteří testují bezpečnost webových aplikací.

Hodnotící kritérium:	*Způsob hodnocení - následující škálou 1 až 4:*
3. Rozsah písemné zprávy	*1=splňuje požadavky,* ***2=splňuje požadavky s menšími výhradami,*** *3=splňuje požadavky s většími výhradami,* *4=nesplňuje požadavky*

Popis kritéria:
Zhodnoťte přiměřenost rozsahu předložené ZP vzhledem k obsahu, tj. zda všechny části ZP jsou informačně bohaté a ZP neobsahuje zbytečné části.

Komentář:
V textu se vykytují prázdné stránky a u některých ilustrací chybí popisky. V kapitole testování bych uvítal ilustrace funkčního řešení. Ačkoliv text pojednává o aplikaci pro příkazovou řádku, důkaz o její funkčnosti v pobobě jejího výstupu by byl v této části textu žádoucí. Funkční aplikace mi byla prezentována až studentem. Bohužel, je zde vidět, že práce byla psána narychlo a proto se zde vyskytují překlepy a jiné typografické nedostatky. Některé pasáže by bylo vhodné stylizovat.

Ocenil bych i rozsáhlejší kapitoly úvod a závěr.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Věcná a logická úroveň práce	*65 (D)*

Popis kritéria:
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.

Komentář:
Text ZP je strukturován dle doporučené šablony. Pasáže týkající se architektury aplikace by mohly být více rozvedeny. K jejímu pochopení by pomohlo, kdyby práce obsahovala více ilustrací a diagramů jednotlivých součástí. Ze stávajícího popisu nemusí být funčnost aplikace zřejmá.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
5. Formální úroveň práce	*65 (D)*

Popis kritéria:
Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 14/2015, článek 3.

Komentář:
ZP je psána v anglickém jazyce. Bohužel je znát, že práce byla psána narychlo (viz bod 3 a 8) a obsahuje větší množství typografických nedostatků a překlepů. V textu se vyskytují prázdné strany a ilustrace bez popisu.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
6. Práce se zdroji	*65 (D)*

Popis kritéria:
Vyjádřete se k aktivitě studenta při získávání a využívání studijních materiálů k řešení ZP. Charakterizujte výběr studijních pramenů. Posuďte, zda student využil všechny relevantní zdroje nebo zda se pokoušel řešit již vyřešené problémy. Ověřte, zda jsou všechny převzaté prvky řádně odlišeny od vlastních výsledků a úvah, zda nedošlo k porušení citační etiky a zda jsou bibliografické citace úplné a v souladu s citačními zvyklostmi a normami.

Komentář:
Práce čerpá z dostatečného množství literatury. Jsou zde obsaženy vědecké články zabývající se PRNG i prameny odkazující na programování pro studentem zvolenou platformu. V referencích není uvedeno datum přístupu k citacím dostupným online. Užití citací v textu by mohlo být častější.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
7. Hodnocení výsledků, publikační výstupy a ocenění	*95 (A)*

Popis kritéria:
Vyjádřete se k úrovni dosažených hlavních výsledků ZP, např. k úrovni teoretických výsledků, nebo k úrovni a funkčnosti technického nebo programového vytvořeného řešení, apod. Případně také zhodnoťte, zda software nebo zdrojové texty, které nevytvořil sám student, byly v ZP použity v souladu s licenčními podmínkami a autorským právem. Popište případnou publikační činnost a získaná ocenění související s řešením této ZP.

Komentář:
Výsledkem práce je funkční prototyp aplikace k prolamování PRNG webserverů využívající PHP. Aplikace může být dále rozšiřována, vužívána komunitou či použita pro srovnání s ostatními podobnými řešeními.

Hodnotící kritérium:	*Způsob hodnocení - nehodnotí se*
8. Komentář o využitelnosti výsledků	

Popis kritéria:
Uveďte, zda hlavní výsledky ZP rozšiřují již publikované známé výsledky a/nebo přinášející zcela nové poznatky. Uveďte možnosti využití výsledků ZP v praxi.

Komentář:
Výslednou aplikaci bude možné použít v praxi v rámci penetračního testování webových aplikací.

Hodnotící kritérium:	*Způsob hodnocení - následující škálou 1 až 5:*
9. Aktivita a samostatnost studenta v průběhu řešení	9a: *1=výborná aktivita,* *2=velmi dobrá aktivita,* ***3=průměrná aktivita,*** *4=slabší, ale ještě dostatečná aktivita,* *5=nedostatečná aktivita* 9b: ***1=výborná samostatnost,*** *2=velmi dobrá samostatnost,* *3=průměrná samostatnost,* *4=slabší, ale ještě dostatečná samostatnost,* *5=nedostatečná samostatnost*

Popis kritéria:
Posuďte, zda byl student během řešení aktivní, zda dodržoval dohodnuté termíny, jestli své řešení průběžně konzultoval a zda byl na konzultace dostatečně připraven (9a). Posuďte schopnost studenta samostatné tvůrčí práce (9b).

Komentář:
Student se velmi aktivně zabývá problematikou bezpečnosti pseudo-náhodných generátorů. Během práce si aktivně vyhledával informace zabývající se problematikou (včetně komunikace se zahraničními výzkumnými skupinami). Informoval mě o své činnosti -- ve většině případů se jednalo o věci implementačního charakteru, ovšem svůj zápal a nadšení do problematiky nebyl schopen proměnit do textové formy k pravidelné kontrole. To se negativně projevilo na kvalitě textu ZP.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
10. Celkové hodnocení	*80 (B)*

Popis kritéria:
Shrňte stránky ZP studenta, které nejvíce ovlivnily Vaše celkové hodnocení. Celkové hodnocení **nemusí** být aritmetickým průměrem či jinou hodnotou vypočtenou z hodnocení v předchozích jednotlivých kritériích 1 až 9.

Text hodnocení:
Výstupem práce je aplikace pro příkazovou řádku, která je schopna nalézt tzv. "seed" pseudo-náhodného číselného generátoru (PRNG) užívaném v PHP webserveru. Cílová skupina uživatelů jsou odborníci pracující v oblasti IT bezpečnosti a penetračního testování. Aplikace se skládá ze dvou hlavních částí. První část (tzv. "Apache Process Pwner") přinutí cílený webserver k vytvoření vlákna, kde lze předvídat seed, a druhá část (tzv. "PRNG Cracker") nalezne seed. Výsledný seed je hledán pomocí hrubé síly (brute-force) a duhových tabulek (rainbow-tables). Funkčnost aplikace byla otestována studentem v laboratorních podmínkách na virtuálním stroji. Ačkoliv mám více výtek k zpracování textu ZP, přihlížím k náročnosti zadání a výsledné aplikaci. Práci hodnotím stupněm B.

Podpis vedoucího práce: