FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Student:	Jaroslav Chládek
Oponent práce:	Ing. Michal Štepanovský, Ph.D.
Název práce:	Feasibility of the Spectre attack in a security-focused language
Obor:	Bezpečnost a informační technologie

Datum vytvoření: 4. 6. 2019

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:
Zadání splněno.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
2. Písemná část práce	*85 (B)*

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:
Rozsah předložené bakalářské práce vzhledem k obsahu odpovídá zvyklostem. Některé pasáže však zbytečně odvádí pozornost a nepovažuji je za důležité (například důkaz teorému 1.4.1 na straně 11, nebo definice průměru a rozptylu na straně 31). Na druhou stranu, větší pozornost by si zasloužila kapitola 1.2 "Branch prediction and speculative execution".

Po věcné stránce je práce v pořádku pouze s několika málo nepřesnostmi. Konkrétně, v popisu algoritmu 1.4.1 na straně 7 v popisu S0 se uvádí, že tato hodnota má být větší než velikost řádky skryté paměti aby se zabránilo důsledkům předvýběru řádek. Nicméně pouhé namapování do jiné řádky tento předvýběr nepotlačí. Ve skutečnosti řadič skryté paměti sleduje dolní bity adresy a předvybírá řádky v rámci dané stránky/rámce. Proto by tato hodnota měla být blízká/rovna velikosti stránky. Tomu odpovídá i zvolená hodnota S0=512, která je již zřejmě dostačující. Dále, v popisu algoritmu 1.4.3 na straně 10 v popisu Tv (čemuž odpovídá kód na řádce 100 přílohy B, strana 49) by mělo být zmíněno, že se jedná především o konstantu, která určuje délku globální historie, která bude vynulována/nastavena do konkrétního stavu. Nejedná se tedy o pouhé zpoždění jak je uvedeno v práci. Zde je na místě zmínit, že tento nedostatek se objevuje i v původním článku představující útok Spectre, ze kterého student vychází. Dále, na straně 26 student uvádí "...the array to remain out of reach of the speculative execution window." Pojem "execution window" není definován a z textu jasně nevyplývá proč Rust zabránil útoku. Bylo by možné procházením celého adresního prostoru přečíst ukrytý textový řetězec? Dále z textu na straně 32 není zcela jasné, zda uváděný rozsah adres je zvolený autorem nebo z něčeho vyplývá. Na straně 33 mohla být explicitně uvedena Null hypotéza a závěr zda se zamítá. Dále na téže straně zcela nerozumím, odkud se vzal interval [0.50, 1.0]. Podobně pro následující kapitoly 4.1.1.2 a 4.1.1.3. V těchto kapitolách zároveň není zřejmé, co znamená "locked/unlocked state". Volba názvů použitých symbolů a dolních indexů v rovnicích 4.1.1.1 až 4.1.2 mohla být více sjednocená a více vypovídající. Dále, poslední odstavec kapitoly 4.5 na straně 41 uvádí možné důvody "selhání" útoku, pokud je úroveň optimalizací nenulová. Zde se domnívám, že hlavním důvodem je vypuštění prázdné smyčky programu (řádek 100 na straně 49) a tedy absence nulování/nastavení globální historie skokových instrukcí. Dále mohla být v práci podrobněji diskutována příloha C.

Co se týče logické struktury práce, jednotlivé kapitoly na sebe plynule navazují. Na straně 29 v poznámce pod čarou je překlep. Má být _mm_lfence.

Co se týče jazykové stránky práce, bakalářská práce je psaná v anglickém jazyce. Zde bych doporučil používat jednodušší formulace. Některé zhutněné výrazy se stávají hůře srozumitelné, například názvy kapitol 4.2 "Implementation output metric choice" a 4.4 "Language binary comparison" apod. Podobě, používání archaických, resp. hovorových slov (například "albeit") by mělo být nahrazeno více frekventovanými - pokud jsou cílovou skupinou i čtenáři s mateřským jazykem jiným než anglickým.

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

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:
Student implementoval útok Spectre v jazyce Rust. K této části práce nemám výhrady.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Hodnocení výsledků, jejich využitelnost	*90 (A)*

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:
Výsledky této práce přináší zajímavý pohled na útok Spectre pomocí programovacího jazyka Rust.

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:
Prosím, vyjádřete se k obrázku 4.1 a rozsahu adres v něm. Z čeho vyplývá rozsah adres? Jak je dlouhý "tajný" textový řetězec?

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
6. Celkové hodnocení	*90 (A)*

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:
I přes některé výhrady, bakalářskou práci považuji za zdařilou a hodnotím ji stupněm A (výborně) a doporučuji k obhajobě.

Podpis oponenta práce: