FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Student:	Bc. Michal Funtán
Oponent práce:	Ing. Tomáš Zahradnický, Ph.D.
Název práce:	Bezpečnostní aspekty Intel Management Engine
Obor:	Počítačová bezpečnost

Datum vytvoření: 2. 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:
Práce měla za úkol provést rešerši dokumentace Intel Management Engine (Intel ME). Student měl nastudovat principy této technologie a jejich omezení. Měl se zaměřit na start systému, moduly Intel ME a jejich závislosti. Dále se měl zaměřit na kryptografické moduly a moduly pro kontrolu integritu kódu. Splnění zadání hodnotím jako s drobnými nedostatky. Nenacházím například vůbec diskuzi o možnostech vypnutí Intel ME prostřednicvím HAP bitu ve flash descriptoru, což v tomto případě považuji za v práci zaměřené na bezpečnostní aspekty jako nedostatek.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
2. Písemná část práce	*70 (C)*

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:
Práce svým rozsahem naplňuje podmínky kladené na diplomovou práci.

Jazyková stránka práce je podprůměrná. Práce obsahuje mnoho anglicismů (nabootovat, bootloader, …) a překlepů (např. dekompresimován a další na str. 33). Jednotky v práci jsou psány nesprávně: 4kiB místo 4 KiB (např. str. 7). Práce pravděpodobně neprošla korekturou před odevzdáním.

Typografická stránka práce je velmi dobrá. Nacházím jen občasné prohřešky typu vytékající slovo (např. v abstraktu) ze zrcadla stránky.

Práce obsahuje popis Intel ME z mnoha různých zdrojů různých verzi Intel ME. To je do jisté míry obtížné, zejména z konzistenčních důvodů. Bohužel práce opomíjí některé důležité aspekty, kterými jsou proces přenosu obrazu Intel ME do firmwaru a možnosti, které při tom jsou. Nejsem si jist, zda byly prováděny nějaké experimenty, zejména pokus s deaktivací Intel ME prostřednictvím High Assurance Platform bitu ve flash descriptoru. V každém případě, tento bezpečnostní aspekt není v práci ani zmíněn, což považuji za nedostatek.

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:

Přílohy práce obsahují různé verze firmwaru a dále text práce.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Hodnocení výsledků, jejich využitelnost	*75 (C)*

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:

Přestože práce obsahuje některé zajímavé závěry, některé věci mi v práci chybí. Nejsem schopen říci, jaké student provedl vlastní experimenty s Intel ME, např. zda ho zkoušel vypnout anebo s ním komunikovat přes HECI. Fakt, že popisuje několik různých verzí firmware dohromady mně způsobovalo občas trochu zmatení. Je také škoda, že o modulu pavp se v práci píše toliko jedenkrát.

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. Jaké vlastní pokusy jste prováděl s Intel ME?
2. Zkoušel jste deaktivovat Intel ME na nějakém Vám dostupném hardwaru?

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
6. Celkové hodnocení	*75 (C)*

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:

Diplomovou práci pana Bc. Michala Funtána doporutučuji k obhajobě a hodnotím ji stupněm C (dobře).

Podpis oponenta práce: