FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Student:	Bc. David Šafrata
Oponent práce:	Ing. Jiří Buček, Ph.D.
Název práce:	Remote Keyless Entry Systems Security Analysis
Obor:	Počítačová bezpečnost

Datum vytvoření: 8. 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:
Zadání bylo 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:
Práce je stručná (s 51 stranami na spodní hranici doporučeného rozsahu), ale obsahuje všechny nezbytné části. Práce je psána srozumitelnou angličtinou, student by se však měl vyhnout použití zkrácených forem (it's). Práci by prospělo zařazení úvodního odstavce do každé kapitoly, aby po názvu kapitoly nenásledoval hned nadpis sekce.

Po věcné stránce práci hodnotím pozitivně. Zejména vyzdvihuji kapitolu 7, popisující studentův nový způsob útoku na dálkové ovládání se šifrou KeeLoq.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
3. Nepísemná část, přílohy	*85 (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:
Práce obsahuje několik skriptů v jazyce Python pro PC a ESP8266 a několik datových souborů. Studentovi musím vytknout, že ve zdrojových textech neuvádí své jméno. Každý skript by měl mít v komentáři označení autora (a datum, instituci, licenci apod.). V případě přejatého kódu ale student odkazuje na zdroj.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Hodnocení výsledků, jejich využitelnost	*95 (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:
Výsledkem studentovy práce je užitečný přehled zabezpečení systémů bezklíčového vstupu používaných zejména v automobilovém průmyslu. Student následně demonstruje vybrané typy útoku na vývojové sadě dálkového ovládání se šifrou Keeloq.

Hlavním přínosem práce je nový útok na přeplnění čítače u šifry KeeLoq, který je kombinací hardwarového přístupu k dálkovému ovládání a opakovacího útoku pomocí softwarově definovaného rádia (SDR).

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:
V kapitole 1.3 uvádíte některé druhy útoků. Jak byste hodnotil tzv. pre-play attack v kontextu své práce?

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
6. Celkové hodnocení	*95 (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:
Student prokázal schopnost samostatné tvůrčí práce. V mém hodnocení převážil přínos studentem vytvořeného nového útoku a přes výše uvedené výhrady diplomovou práci hodnotím známkou výborně.

Podpis oponenta práce: