



Posudek oponenta závěrečné práce

Student: Bc. Jana Ernekerová
Oponent práce: Ing. Viktor Černý
Název práce: Analysis and detection of KRACK attack against WiFi infrastructure
Obor: Počítačová bezpečnost

Datum vytvoření: 31. 1. 2019

<i>Hodnotící kritérium:</i>	<i>Způsob hodnocení – následující škálou 1 až 4:</i>
1. Splnění zadání	<u>1=zadání splněno,</u> 2=zadání splněno s menšími výhradami, 3=zadání splněno s většími výhradami, 4=zadání nesplněno
<i>Popis kritéria:</i> 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.	
<i>Komentář:</i> Téma práce považuji za velmi náročné. Vyžadovalo nastudování velkého množství materiálů a použití velmi specifického hardwaru. Cílem bylo zreplikovat útoky na zranitelnost protokolu během autentizační fáze a jejich následná detekce.	
<i>Hodnotící kritérium:</i>	<i>Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):</i>
2. Písemná část práce	92 (A)
<i>Popis kritéria:</i> 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.	
<i>Komentář:</i> Text práce je psán velmi věcně a srozumitelně. Neobsahuje žádné zbytečné části a je velmi kvalitně očitován. Našel jsem pouze několik drobných nejasností a nedefinovaných zkratek, ale u popisu tak náročného problému je velmi těžké se vyvarovat podobných chyb. Všechny nejasnosti se mi podařilo vysvětlit díky citovaným zdrojům. Na textu naopak oceňuji, jak pečlivě jsou útoky popsány a analyzovány.	
<i>Hodnotící kritérium:</i>	<i>Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):</i>
3. Nepísemná část, přílohy	75 (C)
<i>Popis kritéria:</i> 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	
<i>Komentář:</i> Výsledná detekce útoků je funkční. Mám však výhrady k opakovatelnosti experimentů. Očekával bych alespoň nějaké schéma pro lepší orientaci a poněkud detailnější popis implementace. Dodané skripty pro jazyk python jsou tak velmi obtížně použitelné pro kohokoliv, kdo by chtěl experiment zopakovat. Dále postrádám uživatelský manuál. Implementovaná utilita sice nepostrádá popis použití, ale rozhodně by chtělo vysvětlit, jak interpretovat textový výstup z této utility.	
<i>Hodnotící kritérium:</i>	<i>Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):</i>
4. Hodnocení výsledků, jejich využitelnost	95 (A)
<i>Popis kritéria:</i> 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:

Celkový výsledek považuji za velmi zdařilý. I přes uvedené výhrady, může tato práce posloužit jako základ pro další navazující projekty, které umožní detekci dalších typů útoku založených na této zranitelnosti.

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 odřádkami).

Otázky:

Nemám žádné otázky.

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:

Práci považuji za velmi zdařilou. Vzhledem k velké náročnosti zadání i přes uvedené výhrady hodnotím nejvyšším možným stupněm.

Podpis oponenta práce: