FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Student: Vanda Hendrychová
Oponent práce: Ing. Jiří Dostál, Ph.D.
Název práce: Rogue Access Point on a WiFi-capable microcontroller
Obor: Bezpečnost a informační technologie

Datum vytvoření: 15. 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:
Studentka splnila zadání.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
2. Písemná část práce	*75 (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:
Text práce je věcný a logicky členěn. Mám výtku k rozsahu textu, který se věnuje implementaci - chybí mi zde podrobnější popis implementace, kapitola tak působí poněkud stručně.

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:
Výsledkem je SW a HW implementace na systému, který se skládá s IoT platforem ESP32. Jedna platforma je master a ovládá několik slave zařízení, které sledují Wi-Fi provoz. Celek tak tvoří škálovatelnný distribuovaný systém.

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:
Výsledek práce je využitelný např. při nepřetržité analýze bezpečnosti Wi-Fi AP. Práce se dá rozšířit o další typy útoků a může sloužit i jako návod pro programování platforem ESP32. Podobné systémy se dají využít na hromadných akcích, kde hrozí zneužití špatně zabezpečených AP.

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) Umožňuje systém monitorovat i sítě komunikující v pásmu 5 GHz?
2) Z jakého důvodu jste nevyužila existující projekty typu aircrack nebo wifite?
3) Jaké útoky byste v případě pokračování v práci ještě doplnila?
4) Jakým způsobem by se daly polohově zaměřit vybrané AP?

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:

Výsledkem je funkční řešení rogue AP, který doplňuje stávající projekty jako např. Wi-Fi Pineapple nebo Kismet. Velice hezká je implementace komunikace mezi master a několika slave zařízeními, která provádějí vlastní monitoring a umožňují tak pracovat v celé šíři přiděleného frekvenčního pásma. Jedinou výtku mám ke stručnější kapitole implementace, která mohla obsahovat více detailů. Nicméně, co není přímo v textu je obsaženo ve zdrojových kódech. Podobné systémy se dají využít na hromadných akcích, kde hrozí zneužití špatně zabezpečených AP.

Práci považuji za zdařilou, hodnotím stupněm A a doporučuji k obhajobě.

Podpis oponenta práce: