Review of Master's Thesis

Student: Venger Adam, Bc.
Title: Black-Box Analysis of Wi-Fi Stacks Security (id 23755)
Reviewer: Orsák Michal, Ing., DCSY FIT BUT

1. Assignment complexity — **average assignment**

Cílem práce bylo vytvořit prostředí pro fuzz testování Wi-Fi stacku. Dosavadní aplikace nešlo využít kvůli problémům s výkonnosti a konfigurovatelností. V prostředí bylo otestováno více zařízení a připraven několik testovacích scénářů. Vytvořit fuzzer je jednoduché, ale práce s MCU a potřeba znalosti protokolů přidává na složitosti. Oceňuji také aktuálnost informací o zranitelnostech a testování.

2. Completeness of assignment requirements — **assignment fulfilled**

Všechny body zadání byly splněny.

3. Length of technical report — **in usual extent**

Rozsah technické zprávy odpovídá požadavkům kladeným na diplomovou práci.

4. Presentation level of technical report — **85 p. (B)**

Technická zpráva je napsána přehledně. Některé sekce jsou však příliš krátké a nejspíš měly být sloučeny případně nahrazeny záznamem ve slovníku pojmů, zejména části v popisu IEEE 802.11. Celkově je ale technická zpráva zdařilá a dobře čitelná. Ale vytknull bych to, že práce obsahuje věci, které se jejího výstupu týkají jen velmi okrajově. Nebo spíše, že čtenáři není vysvětleno, jaká je korelace mezi teoretickou částí a možnostmi pro fuzzing.

5. Formal aspects of technical report — **85 p. (B)**

Po jazykové stránce je práce velmi dobře zpracována. Vytvořený text má charakter odborného textu, je dobře čitelný a snadno pochopitelný. Po typografické stránce je práce velmi dobrá, zejména s ohledem na to, že je psaná v angličtině.

6. Literature usage — **85 p. (B)**

Přestože citovaná literatura je převážně v online podobě v této oblasti je to často jediný způsob jak odkázat na aktuální informace. Studijní prameny jsou proto voleny vhodným způsobem a jsou i v textu správným způsobem citovány.

7. Implementation results — **80 p. (B)**

Výsledná sada programů je napsána přehledně a je otestovaná v rámci možností. Avšak podpora protokolů potažmo rámců je omezená, omezené jsou i možnosti scénáře testu. Jak bylo ale v práci zmíněno přidat podporu pro všechny používané zprávy a celé protokoly je velmi časově náročné. Ale ocenil bych, kdyby byl před připraven scénář alespoň pro celý běh autentizace.

8. Utilizability of results

Výsledné prostředí má očekávanou funkcionalitu a je alespoň v částečně rozšiřitelné. Během práce se objevila jedna potenciální chyba v komerčním zařízení, ale může se jedna o formu ochrany. Práce jako taková nepřináší nové poznatky, ale lze ji teoretiky použít ke generování publikačně zajímavých výsledků.

9. Questions for defence

1. Probíhá fuzzing i na úrovni zpráv a nebo jen na úrovní polí zprávy?
2. V práci zmiňujete, že váš fuzzer musí odpovědět do 10ms a že to zvládne do 7ms, co se během tohoto času musí stihnout provést?

10. Total assessment — **80 p. very good (B)**

Práci hodnotím jako zdařilou. Student vytvořil testovací prostředí, které teoreticky obsahuje vše nutné. V tomto testovacím prostředí připravil několik testovacích běhů a otestoval jimi několik zařízení, přičemž se mu možná povedlo objevit chybu v komerčním zařízení. Celá práce vznikla ve spolupráci s firmou, která vyrábí ASIC s Wi-Fi. Technická zpráva má požadované náležitosti a obsahuje aktuální informace z daného oboru.
Proto navrhuji hodnocením stupněm B (velmi dobře).

In Brno 8 June 2021

Orsák Michal, Ing.
reviewer