Review of Master's Thesis

Student: Rusiňák Petr, Bc.
Title: Secure Provisioning of IoT Devices (id 23754)
Reviewer: Hujňák Ondřej, Ing., DITS FIT BUT

1. Assignment complexity **average assignment**

Zadání považuji za průměrně obtížné, vyžaduje nastudování problematiky připojování IoT zařízení do sítě, specifik ESP čipů a ESP-NOW protokolu a implementaci protokolu pro připojování ESP zařízení do WiFi sítí. **Student si však problematiku značně zjednodušil.**

2. Completeness of assignment requirements **assignment fulfilled with minor reservations**

Zadání považuji za splněné, ale v state-of-the-art IoT provisioning protokolů mi **chybí přehled řešení provisioningu u non-IP IoT** protokolů (LoRaWAN, Zigbee, Bluetooth).
Dále nemohu posoudit, **zda byl splněn bod 2d**, protože technická zpráva neobsahuje informaci o požadovaném prototypu.

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

Práce čítá zhruba **75 normostran**, obsahuje však **velké množství výplňového textu**. Například odstavec v každé kapitole obsahující strukturu a přehled podkapitol mne časem až iritoval. Student věnuje velkou pozornost trivialitám a **složitější části popisuje často nedostatečně** (např. fungování Wi-Fi Easy Connect jsem byl nucen dostudovat z oficiálního zdroje). Kapitolu 5.8 zabývající se šifrováním úložiště a secure boot považuji z hlediska návrhu provisioning protokolu za **nadbytečnou**.

4. Presentation level of technical report **62 p. (D)**

Struktura kapitol je **logická** a **vhodně na sebe navazuje**, v rámci kapitol jsou však až příliš často používány dopředné i zpětné křížové odkazy, což znesnadňuje orientaci zejména v tištěné práci. Jak již bylo zmíněno u rozsahu, práce je rozvláčná a **věnuje přílišnou pozornost trivialitám** a některé **složitější části jsou pro čtenáře z textu hůře pochopitelné**.
Schémata jednotlivých fází Wi-Fi Easy Connect v kapitole 4 (Fig. 4.3-4.5) nepřináší proti celkovému schématu (Fig. 4.2) **žádnou přidanou hodnotu**. **Tab. 8.1 má špatný titulek**, co tabulka obsahuje lze ale zjistit z textu na předchozí straně.

5. Formal aspects of technical report **73 p. (C)**

Po **typografické stránce nemám k práci výhrad**, student vhodně doplňuje text ilustracemi a tabulkami. Pouze prostředí *listing*, zejména v kapitole *8 Implementation*, splývá s okolním textem a bylo by vhodné jej vizuálně oddělit, například rámečkem.
Práce je psána anglicky, **obsahuje však některé překlepy a gramaticky špatné fráze** či věty, které by šly odstranit následným čtením a korekturou. (Např. str. 31 věta "... if does not match the original..." neobsahuje podmět, str. 40 "... public key needs to passed .." zase sloveso)

6. Literature usage **75 p. (C)**

Práce obsahuje celkem 33 citovaných zdrojů, které zahrnují **9 vědeckých publikací** a jeden publikovaný standard. Student cituje velké množství manuálů k ESP32, například **6 citací různých částí API** lze zahrnout do jedné citace. Při citování návrhu standardu Wi-Fi Easy Connect student odkazuje na přehledovou stránku se základními marketingovými informacemi. Vzhledem k důležitosti tohoto standardu pro tuto práci by bylo vhodnější **citovat přímo danou specifikaci**.

7. Implementation results **58 p. (E)**

Realizační výstup je funkční a schopen poskytnout zařízením údaje k Wi-Fi síti pomocí ESP-NOW protokolu.

Implementovaný protokol je **navržen jako proof-of-concept**, kdy nebylo hleděno na přílišnou **efektivitu protokolu** (pro typ zprávy vyčleněno 10B, když existuje 6 typů zpráv; vlastní implementace fragmentace zasílá v každém fragmentu celkovou velikost zprávy), protokol není ani částečně kompatibilní s žádným známým provisioning standardem a celý protokol v zásadě **pouze ověřuje použitelnost asymetrické kryptografie**.

Vzhledem ke způsobu implementace stavového automatu lze na koncové zařízení používající tento protokol k připojení do sítě provést **DoS útok**, který mu zamezí v přístupu k síti.

Implementace neumožňuje dynamické změny, a tedy pro přidání nového koncového zařízení (jeho veřejného

klíče) je **nutný re-flash *konfigurátoru***.

Kód je dělen do pěti modulů podle logických operací, je **dostatečně a vhodně komentován**. Student nepopisuje **žádné systematické testování** a validaci provedl pouze úvahou v kapitole 9 Evaluation.

8. Utilizability of results

Práce navrhuje nový protokol pro inicializaci Wi-Fi připojení velmi volně inspirovaný návrhem Wi-Fi Easy Connect standardem. Protokol je redukován na challenge-response autentizaci výměnou asymetricky šifrovaných náhodných čísel a zaslání přístupových údajů chráněných toutéž asymetrickou šifrou. Implementace je použitelná pro jednorázovou inicializaci většího množství zařízení, jeho **úprava pro alespoň částečnou kompatibilitu s některým standardem by však vyžadovala zásadní změny**.

9. Questions for defence

- Z jakého důvodu navrhujete zcela nový provisioning protokol a neimplementoval jste např. podmnožinu protokolu Wi-Fi Easy Connect, který rozebíráte?

10. Total assessment

63 p. satisfactory (D)

Student sice splnil zadání práce, **realizační výstup má však nedostatky**, které znesnadňují jeho další využití. **Technickou zprávu považuji za průměrnou**, celkově tedy hodnotím **stupněm D**.

In Brno 8 June 2021

Hujňák Ondřej, Ing.
reviewer