Supervisor assessment of Master's Thesis

Student: Rusiňák Petr, Bc.
Title: Secure Provisioning of IoT Devices (id 23754)
Supervisor: Malinka Kamil, Mgr., Ph.D., DITS FIT BUT

1. **Assignment comments**
   Jedná se o zadání řešené ve spolupráci s firmou Espressif. Jedná se o průměrně obtížné zadání, které se snaží řešit problematiku zprovoznění IoT zařízení. Součástí práce bylo i využití a testování na infrastruktuře poskytnuté Espressif. Všechny body zadání jsou splněny v alespoň základní kvalitě. Pozitivně hodnotím, že je práce vypracována v angličtině.
2. **Literature usage**
   Student aktivně vyhledával relevantní dostupnou literaturu a vhodně ji začlenil do své práce.
3. **Assignment activity, consultation, communication**
   Student pravidelně komunikoval se mnou i zástupcem firmy během celé doby řešení práce a průběžně vyjasňoval sporné a nejasné body. Zpoždění nastalo až v posledních cca 2 měsících, což se výrazněji projevilo v kvalitě textové části i implementace.
4. **Assignment finalisation**
   Dokončování probíhalo v časové skluzu, kdy došlo ke zpoždění jak v implementaci, tak přípravě textové části. Možnost zásahů do výstupů tak byla omezená.
5. **Publications, awards**
   Student se zúčastnil studentské konference Excel@FIT 2021.
6. **Total assessment** **good (C)**
   Hodnocení práce je ovlivněno hlavně sníženou responzivností během závěrečných fázi práce. Výsledek pak obsahuje značná návrhová zjednoduššení. Nicméně výsledně práci hodnotím dobře.

   Dále přikládam vyjádření zástupce f. Master Internet (Martin Vychodil):
   Software part of the diploma thesis was unfortunately supplied few days before the deadline, thus there was very limited space for detailed discussion on specific implementation points. Generally, the code seems doing expected job - however, the design and code quality could have been way better.
   Few weak points I couldn't miss:

   - *device configuration records: why we need to keep SSID/user/pwd per device? Those settings are global per WiFi instance. In case the configurator would work as a general configuration point for any user network, it's missing a channel field (assuming other networks overlapping with the configurator's one)*
   - *WiFi channel is fixed for all participants - very limiting for real deployment, though I understand it makes the development easier. Proper approach: the device scans all available channels and looks for its configurator one by one*
   - *the code for STATION mode (==enrollee) should be flashed to 'factory' partition, for obvious reasons. However, it seems handled as a common application firmware... in the end, whole target application deployment/upgrade scheme is unclear*
   - *ESP-NOW is used unencrypted - why so? The protocol uses 128-bit encryption (symmetric) which would increase overall security level*
   - *The code contains quite a lot of places without sanity checks - typically for input param pointers. It's correct to let an embedded application crash to figure out the issue, however, sometimes it's sufficient/desired just to log an error and avoid null-pointer touching. This application should be as stable as possible to provide smooth and reliable provisioning. Therefore I'd expect more care regarding faulty conditions*

   Summary: the code is acceptable, however, security applications should be implemented more precisely and conservatively.

In Brno 8 June 2021

Malinka Kamil, Mgr., Ph.D.
supervisor