# Posudek práce

**předložené na Přírodovědecké fakultě JU**

☐ posudek vedoucího ☑ posudek oponenta
☐ bakalářské práce ☑ diplomové práce

| | |
|---|---|
| Autor/~~ka~~: | **Bc. Ondřej Filip** |
| Název práce: | **Analýza zranitelnosti MQTT protokolu s důrazem na chybnou implementaci brokeru** |
| Studijní program a obor: | Aplikovaná informatika |
| Rok odevzdání: | 2020 |

| | |
|---|---|
| Jméno a tituly ~~vedoucího~~/oponenta: | Ing. Marta Vohnoutová |
| Pracoviště: | Ústav aplikované informatiky |
| Kontaktní e-mail: | mvohnoutova@prf.jcu.cz |

**Odborná úroveň práce:**
☐ vynikající ☑ velmi dobrá ☐ průměrná ☐ podprůměrná ☐ nevyhovující

**Věcné chyby:**
☐ téměř žádné ☑ vzhledem k rozsahu přiměřený počet ☐ méně podstatné četné ☐ závažné

**Výsledky:**
☑ originální ☐ původní i převzaté ☐ netriviální kompilace ☐ citované z literatury ☐ opsané

**Rozsah práce:**
☑ veliký ☐ standardní ☐ dostatečný ☐ nedostatečný

**Grafická, jazyková a formální úroveň:**
☐ vynikající ☑ velmi dobrá ☐ průměrná ☐ podprůměrná ☐ nevyhovující

**Tiskové chyby:**
☐ téměř žádné ☑ vzhledem k rozsahu a tématu přiměřený počet ☐ četné

**Celková úroveň práce:**
☐ vynikající ☑ velmi dobrá ☐ průměrná ☐ podprůměrná ☐ nevyhovující

**Slovní vyjádření, komentáře a připomínky vedoucího/oponenta:**

Vyzrálý projev, přehledná úprava, práce je zajímavá a čtivá. U OWASP 10 for IoT by bylo dobré uvést nějaké členění IoT zařízení ve vztahu k OWASP. Určitě ne všechny IoT zařízení mají všechny zranitelnosti. Co jsem v práci poněkud postrádala bylo rozdělení zranitelností a slabých míst podle:

- MQTT protokol – jeho slabosti a zranitelnosti
- MQTT broker – jeho slabosti a zranitelnosti – při předpokladu, že v konfiguraci nebyly chyby (správné nastavení)
- MQTT broker – příklady špatného nastavení a jeho vliv na zranitelnosti
- Jak se mají pokrýt zranitelnosti, které MQTT protokol a MQTT broker z principu pokrýt nemohou. Např. uvádíte, že MQTT broker umí filtrovat zprávy mezi klienty apod. Na základě čeho umí vámi vybraný MQTT broker filtrovat zprávy.

Bylo by instruktivní, vidět to ve formě tabulek a případně schémat.
Ne, že by v práci popsány nebyly, ale ta přehlednost mi tam chyběla. Nový plnohodnotný framework MQTTSA, jehož cílem je asistovat vývojářům při konfiguraci zabezpečení brokeru by mohl být v práci lépe popsán.
Za autorem je spousta studia i práce, což je v práci vidět. I přes drobné námitky jde o kvalitní a zajímavou práci.

**Případné otázky při obhajobě a náměty do diskuze:**

1. Str.7 – „Při vývoji bezpečnostních mechanismů, které mají být použity v zabezpečené síti, odpovědnost zvyšuje nadbytečnost a odpovědnost za provedení určité akce. Odpovědnost zajišťuje správné fungování ostatních bezpečnostních mechanismů.“ – vysvětlete – především tu nadbytečnost.

2. V práci jsou zmíněny nové bezpečnostní výzvy IPv6 – popište, jaké to jsou.
3. Můžete popsat návrh nastavení MQTT brokeru (Mosquitto) jednotlivým útokům bránit, a u kterých útoků je již nutné pokrýt útoky jiným způsobem, např. architekturou sítě, šifrováním atd. např OWASP 10 IoT vs. MQTT broker v rukou zkušeného admina.
4. Kap.2.2.1 – **autorizovaný** klient – jak mám tomu rozumět?
5. Aktualizace koncových IoT zařízení, jak se může MQTT broker bránit útokům tohoto typu?
6. Kap. 3.2.4 - Detekce neobvyklého chování – je podporována MQTT brokerem nebo jak zmíněnou detekci neobvyklého chování nasadíte?
7. Autor tvrdí, že jeho poznatky v této práci mohou posloužit pro zlepšení MQTTSA – buďte konkrétní – jaké?

**Práci**
☑ doporučuji
☐ nedoporučuji
uznat jako diplomovou/~~bakalářskou~~.

**Navrhuji hodnocení stupněm:**
☑ výborně ☐ velmi dobře ☐ dobře ☐ neprospěl/a

**Místo, datum a podpis ~~vedoucího~~/oponenta:**
V Českých Budějovicích dne 24. června 2020