Review of Bachelor's Thesis

Student: Manoilov Ivan
Title: Visualization System of Network Forensic Data (id 23888)
Reviewer: Ryšavý Ondřej, doc. Ing., Ph.D., DIFS FIT BUT

1. **Assignment complexity** — **average assignment**
   Jedná se o středně obtížné zadání.
2. **Completeness of assignment requirements** — **assignment fulfilled**
   Veškeré požadované body zadání byly bez výhrad v práci splněny. Text práce popisuje všechny dílčí aktivity a výsledky požadované zadáním.
3. **Length of technical report** — **in usual extent**
   Rozsah práce odpovídá obvyklému rozsahu kladenému na bakalářskou práci. Některé kapitoly jsou však dosti krátké.
4. **Presentation level of technical report** — **65 p. (D)**
   Práce má logickou strukturu a jednotlivé kapitoly na sebe navazují. Rozsah kapitol je však nevyvážený a to zejména v první části práce. Zde jsou popisovány základní principy, které často nejsou dostatečně vysvětleny, nebo se uvádí zbytečné detaily. Příkladem je kapitola 3, ve které jsou uvedeny různé diagramy. Základní diagramy jsou poměrně detailně vysvětleny, zatímco netradiční diagramy, například Sankey diagram nebo Chord diagram, jsou uvedeny velmi stručně. Obdobné platí pro kapitolu 4. Zde je velmi stručně uveden přehled existujících nástrojů, kdy ovšem není úplně jasné, jaký je jejich význam pro předkládanou práci, například NetworkMiner. Naopak v kapitole 5 je uveden návrh systému, jenž poskytuje dostatečné množství informací pro pochopení principů navrženého řešení. I zde se však objevují nedostatky. Například v obrázku 5.3 je ukázáno databázové schéma, nejsou však pro jednotlivé entity uvedeny jejich atributy. Celkově je práce pochopitelná, nicméně pro lepší hodnocení by byla nutná výraznější úprava textu.
5. **Formal aspects of technical report** — **75 p. (C)**
   Textová část práce je psána v angličtině. Text je srozumitelný, ale věty jsou často kostrbaté a místy se objevuje použití nevhodných či nepatřičných slov. V rozšířeném abstraktu se objevují drobné chyby či některé nepřesnosti. Formální úprava textu je v pořádku.
6. **Literature usage** — **100 p. (A)**
   Autor použil většího množství literárních zdrojů ve své práci. Převzaté informace jsou řádně označeny.
7. **Implementation results** — **85 p. (B)**
   Výstupem je softwarový nástroj pro zpracování a vizualizaci souborů se zachyceným síťovým provozem. Tento nástroj představuje netriviální implementaci, která se skládá z několika modulů, jenž navzájem spolupracují. Studentovi se podařilo vytvořit funkční systém, který velmi dobře demonstruje možnosti vizualizace síťových dat. Přestože má implementace ještě daleko do hotového řešení, je navržena a realizována takovým způsobem, že umožňuje další úpravy a vývoj. Systém navíc poskytuje možnost přidávat další typy vizuálních komponent, v čemž spatřuji jeho velkou výhodu.
8. **Utilizability of results**
   Vytvořený výsledek a to zejména jeho realizační část se může stát základem pro další rozvoj a základem pro řešení, které je možné prakticky nasadit pro vizualizaci síťového provozu.
9. **Questions for defence**
   - Můžete prosím demonstrovat význam Sankey diagramu pro vizualizaci síťových dat? Pro jaká data je tento diagram vhodný a proč?
   - Pro zpracování zachyceného provozu používáte knihovny libpcap, která poskytuje pouze základní operace nad pakety. Proč jste nepoužil nějakou jinou pokročilejší knihovnu, která umí extrahovat také informace z aplikačních protokolu, například ze systému BRO?
10. **Total assessment** — **75 p. good (C)**
    Výsledné hodnocení bere v úvahu rozdílnou kvalitu textové a realizační části. Zatímco realizační část je velmi dobře zpracována a vytvořený nástroj je možné použít pro demonstraci navržených principů a dále jej rozvíjet, textová část má kolísající úroveň a je v ní množství chyb, které by pro lepší hodnocení bylo nutné odstranit.

In Brno 31 May 2021

Ryšavý Ondřej, doc. Ing., Ph.D.
reviewer