MASTER’S THESIS REVIEW

Author:	Bc. Pavla Koháková
Thesis Title:	**Prototype of Application for Rapid Security Incident Investigation**
Thesis Supervisor:	Ing. Ondřej Vaněk, Ph.D.
Thesis Opponent:	Ing. Miroslav Macík, Ph.D.

Assignment

The assignment of the thesis was to analyze and discuss current approaches and tools used by cybersecurity incident analysts, collect their needs and summarize the main features required. The primary aim was to design a prototype of an application user interface for exploring data collected by a security information and event management system as well as from other relevant sources. The goal was to lower the required amount of effort of the cybersecurity analysts. Part of the assignment was a requirement to create and evaluate low and high fidelity prototypes.

Technical Manuscript

The thesis is written in proper English; it is structured into six main chapters. The main content of the thesis is on 62 pages. There are 50 references (mostly online sources).

The analytical part of the manuscript focuses on the target domain; most of the content consists of a user study with seven participants - cybersecurity analysts. The user study is comprehensive and detailed. It is followed by a review of state of the art in the domain. For both, the user study and the state of the art analysis, I miss a conclusion or a summary with generalized outcomes.

Part 3 focuses on the design of the application and its user interface. There are two personas introduced. However, there is no apparent connection to data from user study or domain analysis. The specification of processes covered by the tool is quite comprehensive. The methods used include HTA, CTT and use case description, scenario specification, and storyboarding. The iterative design process is based on the user-centered design method [1].

There are three development phases - a mock-up, a low fidelity prototype, and a high-fidelity prototype. In each phase, the particular prototype has been evaluated using appropriate methods (lo-fi n=5, hi-fi n=6). Some questions in the post-test interview of the low-fidelity prototype evaluation were close-ended (questions 1, 3, 4), which can limit the quality of feedback. I miss a summary of the results of the evaluation.

The manuscript has the following formal issues:

- Almost all figures are not referred from the text.
- In many cases, there are missing summarizing and introductory paragraphs. It makes the text quite hard to read.

Implementation

The implementation has a form of an interactive high fidelity prototype developed in Axure. It reflects the assignment and servers well for evaluation of the high-fidelity prototype.

Questions

1. In section 5.1.1, you propose organizing a focus group aiming at the redesign of Observed entities section and related graphs. Have you organized it? What was the outcome?

Master's thesis of Pavla Koháková is an example of successful application of user-centered design method [1]. The assignment was demanding as the target domain is complex a requires significant effort to gain necessary insight. The manuscript shows the proper development of a specialized application for user group with specific requirements. Minor drawbacks are affecting the clarity of the manuscript that makes it harder to read (see above).

I assess the thesis with mark B (very good).

In Prague, June 4th, 2019

Ing. Miroslav Macík, Ph.D.

References

[1] DIS, ISO. (2009). 9241-210: 2010. Ergonomics of human system interaction-Part 210: Human-centred design for interactive systems.