

INFORMATION OF THE DISSERTATION

Title: **INFORMATION VISUALIZATION IN WEB APPLICATION SECURITY**

Major: **COMPUTER SCIENCE**

Major code: **62.48.01.01**

PhD student: **DANG TRAN TRI**

Scientific advisors: **ASSOC. PROF. DANG TRAN KHANH, PROF. JOSEF KÜNG**

University: **University of Technology – Vietnam National University Ho Chi Minh City**

Dissertation summary

Web-based applications is one of the most popular platforms for developing and deploying software. However, that popularity also makes web applications one of the main targets of Internet's attacks. At the same time, recent researches on web application security tend to focus on automating security processes, thereby removing the roles of security administrators from related tasks. Seeing human's roles as essential parts of the whole security system, this thesis studies and develops models, designs, and techniques to improve security administrators' abilities to secure web applications by applying two main methods: information visualization and human computer interaction. The advantage of this approach is both computing power and human reasoning skill are exploited together. In this thesis, category theory is used to model the information visualization process. Based on that, the thesis has developed a quantitative evaluation method for proposed visualization techniques. This is the first main contribution of the thesis. The second main contribution of the thesis is the review, design, implement, and experiment of some visualization techniques in supporting particular web application security tasks. The last, but not least, main contribution of this thesis is introducing a taxonomy of information visualization methods in web application security domain. This taxonomy can be used to position techniques developed in the future, as well as research problems that lack attention. There are still remaining issues in the thesis which can be improved in the future. Two notable problems are the experiment participants are not representative enough, and experiment data need to be more realistic.

Main contributions

- Theoretical contribution: this dissertation has applied category theory as the foundation to model information visualization process for web application security. Based on that model, a quantitative evaluation technique has been developed to measure information visualization solutions.
- Methodology contribution: this dissertation has developed a taxonomy of information visualization techniques for securing web applications. Based on this taxonomy, it is possible to position future information visualization techniques having the same purpose. Moreover, this taxonomy also helps point out missing research problems in this area.
- Technical contribution: this dissertation has proposed, designed, implemented, and evaluated some specific information visualization techniques to support administrators in securing web applications. Based on experiment results, the supports of these techniques have been confirmed.

Further works

- Theoretical work: more work is required to clarify the application of category theory in security visualization problems. For example, more detailed requirements about identity morphism are needed to determine main objects in the security process, such as web application, input data, administrator, etc. in an objectively and uniquely manner.
- Technical work: a unification framework is required to integrate proposed techniques and solutions into one common systems. This integration may bring more benefits, which do not exist in separate solutions, to users.

Scientific advisor

PhD student

Assoc. Prof. Dang Tran Khanh

Dang Tran Tri