THESIS TITLE	SECURITY ANALYTICS MODEL AND VISUALIZATION OF ONLINE SOCIAL NETWORKS SECURITY USING DATA MINING AND GRAPH-BASED STRUCTURE TECHNIQUE
KEY WORDS	ONLINE SOCIAL NETWORKS, SECURITY ANALYTICS MODEL, VISUALIZATION, DATA MINING, GRAPH THEORY
STUDENT	MRS. PRAJIT LIMSAIPROM
THESIS ADVISOR	DR.PILASTPONG SUBSERMSRI
THESIS CO-ADVISOR	ASSOC.PROF.DR.PRASONG PRANEETPOLGRANG
LEVEL OF STUDY	DOCTOR OF PHILOSOPHY PROGRAM IN INFORMATION TECHNOLOGY
FACULTY	SCHOOL OF INFORMATION TECHNOLOGY SRIPATUM UNIVERSITY
YEAR	2014

ABSTRACT

The objectives of this research are four main points included 1. To analysis for anomaly and attack opportunity in online social networks 2. To study the information diffusion of anomaly and attack patterns in online social networks 3. To identify the influencing nodes which diffuse the anomaly and attack behavior in online social networks and 4. To predict the attacked nodes that may be affected by the anomaly and attack in online social networks, to notify in advance

The research methodologies are Social Network Analysis: SNA, Data Mining: Unsupervised Learning with Cluster Analysis and Supervised Learning with oneR Algorithm of Classification Analysis. The attack log databases of National Blood Transfusion Services Organization and International Healthcare Organization, which collaborative the provided databases in this research is used to analyse the research results. The results of attack log database in the year 2011 – 2013, which present as follows 1. The anomaly and attack patterns are detected with unexpected network communication 16.10%, anomaly with HTTP 12.85% and information

disclosure: attackers gain full path information of the document root on the victim system 12.30% 2. The visualization of information diffusion presents in-degree nodes, which adopt the anomaly and attack behavior in online social networks. Besides, out-degree nodes, which diffuse the anomaly and attack behavior in online social networks. The closeness nodes of in-degree nodes and out-degree nodes in online social networks may be attacked with the anomaly and attack behavior 3.The influencing nodes to adopt and diffuse the anomaly and attack patterns in online social networks are identified with in-degree nodes and out-degree nodes, respectively which adopt or diffuse the anomaly and attack behavior in online social networks and 4. The attacked nodes that may be attacked with anomaly and attack behavior in online social networks, to notify in advance.

The methodology to identify attacked nodes that may be attacked with anomaly and attack behavior in online social networks is found in this research. The closeness nodes of out-degree nodes in online social networks may be attacked with the anomaly and attack behavior of such out-degree nodes. Especially, the accuracy of security analytics model and visualization of online social networks security using data mining and graph-based structure technique to support four objectives of this research is analyzed, and the accuracy of this model is significance with 95% confidence interval to present the useful for analysis the links creation of various large-scale and complex online social networks.