University of Victoria | Graduate Studies

Notice of the Final Oral Examination
for the Degree of Master of Applied Science

of

JAIMIN MODI

BEng (Gujarat Technology University, 2014)

“Detecting Ransomware in Encrypted Network Traffic Using Machine Learning”

Department of Electrical and Computer Engineering

Thursday, August 22, 2019
11:15 A.M.
Engineering Office Wing
Room 430

Supervisory Committee:
Dr. Issa Traoré, Department of Electrical and Computer Engineering, University of Victoria (Supervisor)
Dr. Kin Fun Li, Department of Electrical and Computer Engineering, UVic (Member)

External Examiner:
Dr. Neil Ernst, Department of Computer Science, UVic

Chair of Oral Examination:
Dr. Rogério de Sousa, Department of Physics and Astonomy, UVic

Dr. David Capson, Dean, Faculty of Graduate Studies

Abstract

Ransomware is a type of malware that has gained immense popularity in recent time due to its money extortion techniques. It locks out the user from the system files until the ransom amount is paid.

Existing approaches for ransomware detection predominantly focus on system level monitoring, for instance, by tracking the file system characteristics. To date, only a small amount of research has focused on detecting ransomware at the network level, and none of the published proposals have addressed the challenges raised by the fact that an increasing number of ransomware are using encrypted channels for communication with the command and control (C&C) server, mainly, over the HTTPS protocol.

Despite the limited amount of ransomware-specific data available in network traffic, network-level detection represents a valuable extension of system-level detection as this would provide early indication of ransomware activities and allow disrupting such activities before serious damage can take place.

To address the aforementioned gap, we propose, in the current thesis, a new approach for detecting ransomware in encrypted network traffic that leverages network connection and certificate information and machine learning. We observe that network traffic characteristics can be divided into 3 categories – connection based, encryption based, and certificate based. Based on these characteristics, we explore a feature model that separates effectively ransomware traffic from normal traffic. We study three different classifiers – Random Forest, SVM and Logistic Regression. Experimental evaluation on diversified dataset yields a detection rate of 99.9% and a false positive rate of 0% for random forest, the best performing of the three classifiers.