University of Victoria | Graduate Studies

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

of

BRIJESH JETHVA

BEng (Gujarat Technological University, 2014)

"A New Ransomware Detection Scheme based on Tracking File Signature and File Entropy"

Department of Electrical and Computer Engineering

Monday, August 19, 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. Mihai Sima, Department of Electrical and Computer Engineering, UVic (Member)

External Examiner:
Dr. Venkatesh Srinivasan, Department of Computer Science, UVic

Chair of Oral Examination:
Dr. Sadik Dost, Department of Mechanical Engineering, UVic

Dr. David Capson, Dean, Faculty of Graduate Studies

Abstract

Ransomware is a type of malware that hijack victims' computers, by encrypting or locking corresponding files, and demanding the payment of some ransom in cryptocurrency for the restoration of the files. The last few years have witnessed a sudden rise in ransomware attack incidents, causing significant amount of financial loss to individuals, institutions, and businesses. In reaction to that, ransomware detection has become an important topic for research in recent years. Currently, there are three types of ransomware detection techniques available in the wild: static, dynamic and hybrid. Unfortunately, the current static detection techniques can be easily evaded by code-obfuscation and encryption techniques. Furthermore, current dynamic and hybrid techniques face difficulties to detect novel ransomware.

In the current thesis, we present an upgraded dynamic ransomware detection model with two new sets of features: grouped registry key operation, and combined file entropy and file signature. We analyze the new feature model by exploring and comparing 3 different linear machine learning techniques: SVM, Logistic Regression and Random Forest. The proposed approach help achieves improved detection accuracy and provides the ability to detect novel ransomware. Furthermore, the proposed approach helps differentiate user-triggered encryption from ransomware-triggered encryption, which allows saving as many files as possible during an attack.

To conduct our study, we use a new public ransomware detection dataset collected at the ISOT lab, which consists of 666 ransomware and 103 benign binaries. Our experimental results show that our proposed approach achieves relatively high accuracy in detecting both previously seen and novel ransomware samples.