Notice of the Final Oral Examination
for the Degree of Doctor of Philosophy

of

MOHAMED ELSAYED

MSc (Ain Shams University, Egypt, 2016)
BSc (Alexandria University, Egypt, 2007)

“Addressing Cybersecurity Threats for Computer Networks”

Department of Electrical and Computer Engineering

Thursday, December 17, 2020
10:00 A.M.
Remote Defence

Supervisory Committee:
Dr. T. Aaron Gulliver, Department of Electrical and Computer Engineering, University of Victoria (Supervisor)
Dr. Issa Traore, Department of Electrical and Computer Engineering, UVic (Member)
Dr. Jens Weber, Department of Computer Science, UVic (Outside Member)

External Examiner:
Dr. Mohammad Zulkernine, School of Computing, Queen’s University

Chair of Oral Examination:
Dr. Stephen Lindsay, Department of Psychology, UVic

Dr. Stephen Evans, Acting Dean, Faculty of Graduate Studies
Abstract

Information technology systems are essential for most businesses as they facilitate the handling and sharing of data and the execution of tasks. Due to the connectivity to the internet and other internal networks, these systems are susceptible to cyberattacks. Computer worms are one of the most significant threats to computer systems because of their fast self-propagation to multiple systems and malicious payloads. Modern worms employ obfuscation techniques to avoid detection using patterns from previous attacks. Although the best defense is to eliminate (patch) the software vulnerabilities being exploited by computer worms, this requires a substantial amount of time to create, test, and deploy the generated patches. Worm containment techniques are used to reduce or even stop the spread of worm infections to allow time for software patches to be developed and deployed. In this dissertation, a novel blockchain-based collaborative intrusion prevention system model is introduced. This model is designed to proactively contain zero-day and obfuscated computer worms. In this model, containment is achieved by creating and distributing signatures for the exploited vulnerabilities. Blockchain technology is employed to provide liveness, maintain an immutable record of vulnerability-based signatures to update peers, accomplish trust in confirming the occurrence of a malicious event and the corresponding signature, and allow a decentralized defensive environment. A consensus algorithm based on the Practical Byzantine Fault Tolerance (PBFT) algorithm is employed in the model. The TLA+ formal method is utilized to prove the correctness, liveness, and safety properties of the model as well as to assert that it has no behavioral error. After the behavioral assertion, a blockchain-based automatic worm containment system is implemented. A synthetic worm is created to exploit a network-deployed vulnerable program, thus evaluating the effectiveness of the implemented containment system. The implemented containment system succeeds in containing the created worm as well as it shows a promising performance results.