PROGRAMME

The Final Oral Examination for the Degree of

DOCTOR OF PHILOSOPHY
(Department of Electrical and Computer Engineering)

Mohamed Elgamal

2004 Cairo University MSc
1996 Benha University BSc

“The Extended Maurer Model: Bridging Turing-Reducibility and Measure Theory to Jointly Reason about Malware and its Detection”

Tuesday, August 26, 2014
10:00 A.M.
David Turpin Building, room A144

Supervisory Committee:
Dr. Stephen W. Neville, Department of Electrical & Computer Engineering, UVic (Supervisor)
Dr. Fayez Gebali, Department of Electrical & Computer Engineering, UVic (Member)
Dr. Issa Traore, Department of Electrical & Computer Engineering, UVic (Member)
Dr. Jens Weber, Department of Computer Science, UVic (Outside Member)

External Examiner:
Dr. Jose Fernandez, Department of Computer Engineering, Polytechnique Montreal

Chair of Oral Examination:
Dr. Kenneth Stewart, Department of Economics, UVic
Abstract

An arms race exists between malware authors and system defenders in which defenders develop new detection approaches and malware authors develop new techniques to bypass them. This motivates the need for a formal framework to jointly reason about malware and its detection in light of this underlying arms race. This dissertation presents such a formal framework termed the extended Maurer model (EMM) and then applies this framework to develop a game-theoretic model of malware authors versus system defenders confrontation. The EMM has been developed as an extension to the existing Turing-reducible Maurer model. The components of Maurer model have been extended to include the necessary structures that enable the modeling of programs, concurrency, multiple processors, and networks. Through the proposed EMM, we provide formalizations for the violations of the standard security policies. Additionally, we also propose formal definitions of a number of common malware classes, including viruses, Trojan horses, spyware, bots, and computer worms. We also show that the proposed EMM is complete in terms of its ability to model all implementable malware within the context of a given defended environment. We then use the EMM to evaluate and analyze the resilience of a number of common malware detection approaches. Additionally, we also use the EMM to formally show that malware authors can avoid detection by dynamic system call sequence detection approaches, which also agrees with recent experimental work. A measure-theoretic model of the EMM is then developed by which the completeness of the EMM with respect to its ability to model all implementable malware detection approaches is shown. Finally, using the developed EMM, we provide a game-theoretic model of the confrontation of attackers and system defenders. Using this game model, under game theory’s strict dominance solution concept, we show that rational attackers are always required to develop malware that is able to evade the deployed malware detection solutions. Moreover, we show that the attacker and defender adaptations can be modeled as a sequence of iterative games. Hence, the question can be asked as to the conditions required if such a sequence (or arms race) is to converge towards a defender advantageous end-game. It is shown via the EMM
that, in the general context, this desired situation requires that the next attacker adaptation becomes, at least, a computationally hard problem. If this is not the case, then we show via the EMM measure theory perspective that the defender is left in need to track statistically non-stationary attack processes.

**Awards, Scholarships, Fellowships**


**Publications**


2. Elgamal, M.; Neville, S. W.; “Assessing the Limits of Situational Awareness within Larger-scale IT Environment”, *In Progress*. 