PROGRAMME

The Final Oral Examination for the Degree of

DOCTOR OF PHILOSOPHY (Department of Computer Science)

Shahid Alam

2007 Carleton University MASc (Electrical Eng)
1999 Wayne State University MSc (Computer Eng)
1990 University of Engineering & Technology Lahore BSc

“A Framework for Metamorphic Malware Analysis and Real-Time Detection”

Wednesday, August 13, 2014
9:00 a.m.
David Turpin Building, room A144

Supervisory Committee:
Dr. R. Nigel Horspool, Department of Computer Science, UVic (Co-Supervisor)
Dr. Issa Traore, Department of Electrical and Computer Engineering, UVic (Co-Supervisor)
Dr. Yvonne Coady, Department of Computer Science, UVic (Member)
Dr. Ibrahim Sogukpinar, Department of Computer Engineering, (Outside Member)

External Examiner:
Dr. Habib Hamam, Department of Electrical Engineering, University of Moncton

Chair of Oral Examination:
Dr. Michel Lefebvre, Department of Physics and Astronomy, UVic
Abstract

Metamorphism is a technique that mutates the binary code using different obfuscations. It is difficult to write a new metamorphic malware and in general malware writers reuse old malware. To hide detection the malware writers change the obfuscations (syntax) more than the behavior (semantic) of such a new malware. On this assumption and motivation, this thesis presents a new framework named MARD for Metamorphic Malware Analysis and Real-Time Detection. We also introduce a new intermediate language named MAIL (Malware Analysis Intermediate Language). Each MAIL statement is assigned a pattern that can be used to annotate a control flow graph for pattern matching to analyse and detect metamorphic malware. MARD uses MAIL to achieve platform independence, automation and optimizations for metamorphic malware analysis and detection. As part of the new framework, to build a behavioral signature and detect metamorphic malware in real-time, we propose two novel techniques, named ACFG (Annotated Control Flow Graph) and SWOD-CFWeight (Sliding Window of Difference and Control Flow Weight). Unlike other techniques, ACFG provides a faster matching of CFGs, without compromising detection accuracy; it can handle malware with smaller CFGs, and contains more information and hence provides more accuracy than a CFG. SWOD-CFWeight mitigates and addresses key issues in current techniques, related to the change of the frequencies of opcodes, such as the use of different compilers, compiler optimizations, operating systems and obfuscations. The size of SWOD can change, which gives anti-malware tool developers the ability to select appropriate parameter values to further optimize malware detection. CFWeight captures the control flow semantics of a program to an extent that helps detect metamorphic malware in real-time. Experimental evaluation of the two proposed techniques, using an existing dataset, achieved detection rates in the range 94% - 99.6% and false positive rates in the range 0.93% - 12.44%. Compared to ACFG, SWOD-CFWeight significantly improves the detection time, and is suitable to be used where the time for malware detection is more important as in real-time (practical) anti-malware applications.

Awards, Scholarships, Fellowships

2013 Graduate Travel Grant, SIN 2013, Aksaray, Turkey
1998-1999 Graduate Professional Scholarship, Wayne State University
1998-1999 Graduate Award, Wayne State University
Presentations


Publications


