University of Victoria | Graduate Studies

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

1. Alam, S. "MARD: A Framework for Metamorphic Malware Analysis and Real-Time Detection." *The 28th IEEE International Conference on Advanced Information Networking and Applications, Research Track - Security and Privacy,* Victoria, B.C., Canada. May 2014. (oral)

2. Alam, S. "MAIL: Malware Analysis Intermediate Language - A Step Towards Automating and Optimizing Malware Detection." The Sixth ACM International Conference on Security of Information and Networks (SIN 2013), ACM Special Interest Group on Security, Audit and Control (SIGSAC), Aksaray, Turkey, Nov. 2013. (oral)

Publications

1. Alam, S.; Horspool, N. R.; Traore, I.; Sogukpinar, I; "A Framework for Metamorphic Malware Analysis and Real-Time Detection." *Elsevier Journal of Computers and Security* **(submitted).**

2. Alam, S.; Sogukpinar, I.; Traore, I; Horspool, N. R.; "Sliding Window and Control Flow Weight for Metamorphic Malware Detection." *Springer Journal of Computer Virology and Hacking Techniques* **2014 (accepted).**

3. Alam, S.; Sogukpinar, I.; Traore, I.; Coady, Y.; "In-Cloud Malware Analysis and Detection: State of the Art." *The Seventh ACM International Conference on Security of Information and Networks*, Glasgow, UK, 9-11 September, **2014 (accepted).**

4. Alam, S.; Horspool, N. R.; "A Survey: Software-Managed On-Chip Memories." *Journal of Computing and Informatics* **2014, (accepted).**

5. Alam, S.; Traore, I.; Sogukpinar, I.; "Current Trends and the Future of Metamorphic Malware Detection." *The Seventh ACM International Conference on Security of Information and Networks*, **2014, (accepted).**

6. Alam, S.; Horspool, N. R.; Traore, I; "MARD: A Framework for Metamorphic Malware Analysis and Real-Time Detection." *Proceedings of the 28th IEEE International Conference on Advanced Information Networking and Applications, Research Track - Security and Privacy,* IEEE Computer Society, **May, 2014.**

7. Alam, S.; "Is Fortran Still Relevant? Comparing Fortran With Java and C++." *International Journal of Software Engineering & Applications,* **2014,** 5 (3) 25-45.

8. Alam, S.; Jackson, L.; "A Case Study: Are Traditional Face-To-Face Lectures Still Relevant When Teaching Engineering Courses." *International Journal of Engineering Pedagogy (iJEP)*, **2013**, 3 (4), 9-15.

9. Alam, S.; "CAL: Using constraints with action language for model evolution." *Journal of Software Engineering*, **2013,** 2 (1)1-8.

10. Alam, S.; Horspool, N. R.; Traore, I.; "MAIL: Malware Analysis Intermediate Language - A Step Towards Automating and Optimizing Malware Detection." *Proceedings of the Sixth ACM International Conference on Security of Information and Networks*, **2013,** 26-28.

11. Alam, S.; "MAIL: Malware Analysis Intermediate Language." *Technical Report, College of Engineering, University of Victoria*, **2013.**

12. Alam, S.; Jackson, L.; "A Case Study: Are Traditional Face-To-Face Lectures Still Relevant When Teaching Engineering Courses." *Proceedings of the IEEE International Conference on Teaching, Assessment and Learning for Engineering (TALE 2013)*, **2013.**

13. Ajila, S. A.; Alam, S; "E-CAL: A formal language for software model evolution." *Proceedings of the 12th IEEE International Conference on Information Reuse and Integration (IRI 2011)*, **2011.**

14. Alam, S.; Horspool, N. R. "Current trends and the future of software-managed on-chip memories in modern processors." *Proceedings of the 2010 International Conference on High Performance Computing Systems (HPCS 2010),* **2010.**

15. Ajila, S. A.; Alam, S; "Using a formal language constructs for software model evolution." *Proceedings of the 3rd IEEE International Conference on Semantic Computing (ICSC 2009),* **2009,** 14-16.

16. Alam, S; Ajila, S. A.; "Using constraints with action language for model evolution." *Proceedings of the 2007 International Conference on Software Engineering Research & Practice (SERP 2007),* **2007.**