University of Victoria | Graduate Studies

PROGRAMME

The Final Oral Examination
for the Degree of

DOCTOR OF PHILOSOPHY
Department of Electrical and Computer Engineering

Soltan Alharbi

2000	Florida Institute of Technology	MSc
1998	Florida Institute of Technology	BSc

Proactive System for Digital Forensic Investigation

Wednesday, March 19, 2014
10:00 AM
DTB A144

Supervisory Committee:
Dr. Issa Traoré, Electrical and Computer Engineering, UVic (Co-supervisor)
Dr. Jens Weber, Computer Science, UVic (Co-supervisor)
Dr. Fayez Gebali, Electrical and Computer Engineering, UVic (Unit Member)
Dr. Afzal Suleman, Mechanical Engineering, UVic (Outside Member)

External Examiner:
Dr. Cungang (Truman) Yang, Electrical and Computer Engineering, Ryerson University

Chair of Oral Examination:
Dr. Linda Welling, Department of Economics, UVic

Abstract

Digital Forensics (DF) is defined as the ensemble of methods, tools and techniques used to collect, preserve and analyze *digital* data originating from any type of digital media involved in an incident with the purpose of extracting valid evidence for a court of law.

DF investigations are usually performed as a response to a digital crime and, as such, they are termed *Reactive Digital Forensic* (RDF). An RDF investigation takes the traditional (or post-mortem) approach of investigating digital crimes after incidents have occurred. This involves identifying, preserving, collecting, analyzing, and generating the final report.

Although RDF investigations are effective, they are faced with many challenges, especially when dealing with anti-forensic incidents, volatile data and event reconstruction. To tackle these challenges, *Proactive Digital Forensics* (PDF) is required. By being proactive, DF is prepared for incidents. In fact, the PDF investigation has the ability to proactively collect data, preserve it, detect suspicious events, analyze evidence and report an incident as it occurs.

This dissertation focuses on the detection and analysis phase of the proactive investigation system, as it is the most expensive phase of the system. In addition, theories behind such systems will be discussed. Finally, implementation of the whole proactive system will be tested on a botnet use case (Zeus).

Awards, Scholarships, Fellowships

1999-2000 – Full tuition waiver for first year of Master's degree, Florida Institute of Technology

1994-2000 – Full scholarship for both Bachelor and Master's degrees, Ministry of Higher Education of Saudi Arabia

Publications

1. Alharbi, S., Weber-Jahnke, J., and Traoré, I. "The proactive and reactive digital forensics investigation process: A systematic literature review". Information Security and Assurance, Springer **2011**, 87-100.

2. Alharbi, S., Weber-Jahnke, J., and Traoré, I. "The proactive and reactive digital forensics investigation process: A systematic literature review". International Journal of Security and Its Applications **2011**, 5(4): 59-72.

3. Alharbi, S., Moa, B., Weber-Jahnke, J., and Traoré, I. "High performance proactive digital forensics". Journal of Physics: Conference Series **2012**, IOP Publishing, vol. 385, page 012003.