Formalising Event Reconstruction in Digital Investigations

Pavel Gladyshev

The thesis is submitted to University College Dublin for the degree of PhD in the Faculty of Science

August 2004

Department of Computer Science

Head of department: Prof. Barry Smyth
Supervisor: Dr. Ahmed Patel

TO MY FAMILY

Contents

List of Figures

Abstract

The highly technical nature of computer crime facilitated the development of a new branch of forensic science called digital forensics. Instead of dead bodies, it collects and analyses data produced, transmitted, and stored by digital devices. The field of digital forensics is rapidly evolving. A major research challenge perceived by the digital forensic community is the need for theoretical basis validating correctness of methods and tools used by digital forensic investigators.

An important part of digital forensic analysis is event reconstruction. It is the process of determining the events that happened during the incident. In digital forensic investigations, event reconstruction is fairly complex. A single push of a button triggers a chain of events inside one or more digital devices that produce the digital evidence. Informal, unaided reasoning is not always sufficient to comprehensively analyse this chain of events.

One way to make event reconstruction more objective and rigorous is to employ mathematics. As a first step in this direction, this research aimed to give formal meaning to the problem of event reconstruction. More specifically, the objectives of this research were (1) to define a formal model of event reconstruction, and (2) to demonstrate that that model can be used as a basis for formalisation and automation of selected examples of digital forensic analysis.

To achieve these objectives, the following approach was adopted. First, a study of digital forensic techniques and legal theory was undertaken to clarify the requirements to and place of event reconstruction in digital forensic analysis. Then, a review of existing event reconstruction techniques was carried out. The review has shown that none of these technique are fully adequate in digital forensic context. Next, a formal model of event reconstruction was defined. The defined model possesses the following features:

- The system under investigation is modeled as a finite state machine.
- A special-purpose formalism called "evidential statement" is used for describing the evidence.
- The outcome of event reconstruction is given precise mathematical meaning in terms of the finite state machine model of the system.

The usefulness of the proposed model was then demonstrated by developing a generic event reconstruction algorithm, based on the defined model, and using that algorithm to formalise and automate selected examples of digital forensic analysis. Finally, several possible directions for future research have been suggested.

Declaration

I declare that this thesis is my own work and has not been submitted in any form for another degree or diploma at this, or any other, University or institute of tertiary education.

Pavel Gladyshev
August, 4 2004