Review of PhD Thesis

Methods for Intelligent Network Forensics

Submitted by Jan Pluskal to the
Faculty of Information Technology
Brno University of Technology
under the supervision of
doc. Ing. Ondřej Ryšavý, Ph.D.

This research focuses on the area of network forensics for Law Enforcement Agencies. This is a current and important area of research. The work is original and very interesting.

The work aims to address the reliability and capability for the capture of complete and incomplete network traffic sessions, and for the analysis of protocols and the associated applications being used on the network under investigation. The architecture for a network forensics tool has also been proposed and developed. Issues concerning tunnelling and overlay networks have been examined and a case study has been analysed.

Chapter 1 presents the goal of the research. The goal has been broken into four objectives. Figure 1.1 graphically maps the overall research focus to the objectives of the work, and demonstrates how it has been addressed in the published articles and papers. The research objectives have been implemented in a network forensics tool called Netfox. While the research objectives are articulated well, there are no clearly stated research questions. A section highlighting the main contributions of the work would be of benefit to the manuscript.

The second chapter presents the state of the art in the area of Network Forensics. The definition of network forensics is accurate and there is a comprehensive review of tools used by network forensic investigators. There are sections covering the objectives of data collection, protocol analysis, tunnelling and big data.

Chapter 3 presents a summary of the research that has been conducted. Each paper is presented and the main contributions are identified. Chapter 4 concludes the dissertation.

The main contributions of the work include

- A method to overcome the inability to extract the remaining data in a TCP conversation when the situation of a missing packet is encountered during the conversation.

- The ability to determine protocols and applications used for communications.

- The feasibility of horizontal scalability for increasing the throughput of capture traffic network processing.

- The identification and analysis of underlying network encapsulation using GSE as a case study.

There are 78 references present in the bibliography. The work has been published on seven occasions overall. These publication are in a number of well respected conferences such as ICDF2C and in high ranking journals such as Elsevier's Forensic Science International: Digital Investigation, and the Journal of Digital Forensics, Security and Law.

I believe that this thesis meets the requirements for the award of the degree of Ph.D.

I commend the author on their work and I recommend the thesis for defence.

Dr John Sheppard,
School of Science and Computing,
South East Technological University of Ireland