DIGITAL FORENSIC INVESTIGATIONS IN THE CLOUD

With software-intensive systems becoming more pervasive, an increasing number of assets, which are transmitted, manipulated, or stored digitally, are being compromised by cyber crimes. To identify and prosecute those responsible for such crimes, a digital forensic investigation aims to collect, analyse and present digital evidence necessary to demonstrate how a digital crime was committed, what harm was done, and who was responsible. Although exiting tools, such Sleuthkit and Encase, can be used to extract digital forensic evidence, investigators still have to approach each crime case from scratch, by postulating potential hypotheses and manually analysing large volumes of data. Traditional digital investigations assume access to and control of IT assets - such as storage - during an investigation, but this may not be the case if system uses volatile storage or a virtualized infrastructure.

In Lero's ManSec project Dr. Liliana Pasquale and Professor Bashar Nuseibeh have been working with IBM Software Labs to develop a framework to support forensic readiness. This framework is based on the design of potential speculative hypotheses of a crime in advance. To preserve necessary - but volatile – evidence generated by volatile sources, such evidence may be collected proactively depending on the likelihood of a crime taking place. If an investigation starts, the evidence already collected is analysed to assess if some of the speculative hypotheses of a crime hold and what further evidence is necessary to support them. The likelihood of each hypothesis is estimated depending on the state of data collected. For each hypothesis that is satisfied, a case is generated, in the form of a structured argument, to demonstrate how the evidence collected supports that hypothesis.

Preliminary results are promising. We are developing an open source toolset to support proactive digital investigations in large distributed systems, which we are using to demonstrate the efficacy of our approach in Cloud computing environments. Liliana Pasquale also received a Microsoft Windows Azure for Research Award entitled "Minority Report: Using the Cloud to Enable Proactive Digital Forensic Investigations". This award will enable the Lero team to investigate performance enhancement to our framework through the use of software parallelisation techniques.
Our aim is to continue evaluating the feasibility of proactive analysis for large systems and to contribute to the development of substantive systems that are forensics-ready.

lero

THE IRISH SOFTWARE
RESEARCH CENTRE