Self-Configuring NetFlow Anomaly Detection using Cluster Density Analysis

Kieran Flanagan*, ***, Enda Fallon*, Abir Awad**, Paul Connolly***

*Software Research Institute, Athlone Institute of Technology, Athlone, Ireland

**Faculty of Computing, Engineering and Science, University of South Wales, UK

***The NPD Group, Inc, IDA Business Park, Athlone, Co. Westmeath, Ireland

k.flanagan@research.ait.ie, efallon@ait.ie, abir.awad@southwalse.ac.uk, paul.connolly@npd.com

Abstract— **The growing number of malicious network attacks has resulted in the need for a fast, reliable method to identify possible malicious activity. For any organization it is critical that confidential and proprietary data is sufficiently secured to address both legal and contractual obligations. The changing nature of security attacks has caused a surge of interest in anomaly detection mechanisms. Such mechanisms are suitable as they can dynamically adapt to changed network conditions and threats without security personnel intervention. While anomaly detection mechanisms have significant potential they are technically limited. Many anomaly detection approaches are unsuitable for real time environments. The approaches also typically operate on the basis of "what is common is normal". Mechanisms are typically singular in focus analyzing data on one specific type. This paper proposes a novel framework to detect anomalies previously hidden within current detection techniques. The approach is easily extensible taking input from many security assessment applications; network traffic, asset criticality. Using time based correlations with historic data; a method for generating a normalized view of activity on the network is achieved. Once normality has been established for specific time intervals an extensible environment is implemented which allows for the active monitoring of anomalies in real-time. Anomalies which had sufficient "commonality" to remain undetected by other mechanisms are identified and analyzed. The proposed solution is completely autonomous, capable of acting independently with no previous knowledge required. The presented results describe NetFlow activity of the NPD Groups' network over a 24-hour period and outline real world anomalies that were detected.**

Keyword— **Anomaly Detection, NetFlow, Clustering, Density Analysis**

Kieran Flanagan received his BSc degree (with honors) in Software Design in 2015. After this, he joined The NPD Group while studying as a postgraduate in Athlone Institute of Technology. He is currently perusing his MSc with his research activities including the creation of abstracted vulnerability metrics for network based assets and the detection of possible malicious network activity.

Dr. Enda Fallon joined Athlone Institute of Technology (AIT) from Ericsson in 2002. In 2003 he founded AIT's Software Research Institute (SRI). Since 2003, Enda has been a principal investigator on over 30 collaborative industry/academic research projects. His research interest focuses on service mediation and adaptation for heterogeneous networking environments. Enda holds a BSc in Computer Science and Mathematics from University College Galway and an MSc in Software Engineering from Athlone Institute of Technology and a PhD (Computer Science) from the Performance Engineering Laboratory at University College Dublin.

Dr. Abir Awad received her PhD degree in Computer Science from Polytech' Nantes, University of Nantes (Nantes, France). Her PhD was within the framework of the research project "ACSCOM", "Chaos based security for mobile communicating systems" supported by the ANRT. She developed her doctoral thesis on Cryptography from September 2006 to November 2009. Later, she joined the Operational Cryptology and Virology Laboratory ((C+V)°), ESIEA and Le Mans University in Laval in 2010 and the computer science lab. (LIFO), University of Orleans in Orleans in 2011 as a lecturer-researcher. In 2012, she worked at the computer science dep, Ryerson University, Toronto, Canada. She is currently working as a researcher at the Software Research Institute (SRI), Athlone Institute or Technology (AIT) within the Irish Centre of Cloud Computing and Commerce IC4).

Paul Connolly started working in the NPD Group in 2014 as a Senior Security Analyst to evaluate and test security applications within the company. His current research focus is on the development of novel risk evaluation and visualization approaches.