Multi Sensor National Cyber Security Data Fusion

Ignus Swart, Barry Irwin and Marthie Grobler

Abstract:
A proliferation of cyber security strategies have recently been published around the world with as many as thirty five strategies documented since 2009. These published strategies indicate the growing need to obtain a clear view of a country's information security posture and to improve on it. The potential attack surface of a nation is extremely large however and no single source of cyber security data provides all the required information to accurately describe the cyber security readiness of a nation. There are however a variety of specialised data sources that are rich enough in relevant cyber security information to assess the state of a nation in at least key areas such as botnets, spam servers and incorrectly configured hosts present in a country. While informative both from an offensive and defensive point of view, the data sources range in a variety of factors such as accuracy, completeness, representation, cost and data availability. These factors add complexity when attempting to present a clear view of the combined intelligence of the data. By applying data fusion the potential exists to provide a comprehensive and representative view of all data sources fused together, regardless of their complexity. This method is not often used in cyber defence systems, since cyber sensor data is typically hard to classify in traditional data fusion techniques due to the diversity and ambiguity present in the sources. This research will examine a variety of currently available Internet data sources and apply it to an adapted Joint Directors of Laboratories (JDL) data fusion model. The model has been adapted to suit national level cyber sensor data fusion with the aim to formally define and reduce data ambiguity and enhance fusion capability in a real world system. The data examined will then be applied to a case study that will show the results of applying available open source security information against the model to relate to the current South African cyber landscape.

Keywords: attack surface, cyber security readiness, JDL model, open source, national security policy, personally identifiable information, sensor fusion