Abstract

Stellar, a system that builds prioritized scenarios from the alerts produced by multiple heterogeneous network defense systems is presented. Stellar runs in realtime, combining the alerts into scenarios and assigning each scenario an evolving security risk. Security risk is assessed by a set of rules written in Security Assessment Declarative Language (SADL), a powerful language that combines network topology, mission, and alert context to evaluate scenario threat. The security risk of a scenario is reassessed each time the scenario changes providing realtime feedback to analysts via a graphical user interface. Experiments on real and synthetic data indicate that Stellar is both scalable and accurate.

* This work is sponsored by the Department of Defense under the Air Force Contract FA8721-05-0002. Opinions, interpretations, conclusions and recommendations are those of the author and are not necessarily endorsed by the United States Government.