The Science of Security Monitoring in Critical Infrastructure Networks

Kartik Palani
University of Illinois at Urbana-Champaign

Abstract

The addition of hosts, both traditional and more modern(programmable switches and IoT nodes), makes computer networks significantly more complex. Added to this, application requirements in terms of latency and bandwidth are becoming more constraining. This rise in complexity, on one hand, increases the attack surface and on another, it means significantly larger logs and harder work for analysts. We hypothesize that it is possible to find an optimal placement of security monitors such that along with the above mentioned constraints, budget requirements are met too. Finding needles in a haystack becomes easier when the hay is blown away.

Our approach involves devising an algorithmic solution to the placement problem. In order to evaluate various placement strategies, we design an open-source simulator-emulator called Melody that generates network traffic under various configurations. Melody is designed to allow network administrators make confident decisions about the security solutions they deploy in their networks.