The Summer Undergraduate Research Fellowship (SURF) Symposium
3 August 2017
Purdue University, West Lafayette, Indiana, USA

Optimal Placement of Intrusion Detection Systems to Identify Multi-Stage Attacks in Software Defined Networks

Rebecca S. Salo, Subramaniyam Kannan, and Paul C. Wood
School of Electrical and Computer Engineering, Purdue University

ABSTRACT

A major threat to network security is the multi-stage attack, where an attacker compromises an outer edge server from which he penetrates an inner server, and so on, until he gains access to protected information deep in the network. Intrusion detection systems (IDS) can detect such attacks, but limited resources constrain the number of IDS deployed. Software defined networking (SDN) provides network flexibility, and combined with network function virtualization (NFV), it enables IDS placement optimizations that can relieve cost constraint pressures. In this work, we develop a novel algorithm for placing IDS to maximize network protection benefits and minimize costs. The benefit of an IDS configuration is given by the probability of reducing an attacker's chance of success, and the corresponding cost includes IDS installation and operational costs. We find the configuration which yields the highest benefit given a cost constraint by using the genetic algorithm for optimization, and we compare its results to exhaustive techniques. For networks with more than 5 servers, the algorithm consistently maintains over 85% of the maximum benefit with its placement of IDS, while keeping costs as low as 30% of the naive complete-coverage cost. The genetic algorithm error is less than 5% when compared to exhaustive techniques; and for networks larger than 10 servers, the genetic algorithm runtime is less than a third of the exhaustive search runtime. Using our solution, network administrators can reduce the costs of protecting their systems from multi-stage attacks.

KEYWORDS

Intrusion detection systems, software defined networks, multi-stage attacks