Security Metrics

The attack graph is an abstraction that reveals the ways an attacker can leverage vulnerabilities in a network to violate a security policy. When used with attack graph-based security metrics, the attack graph may be used to quantitatively assess security-relevant aspects of a network. The Shortest Path metric, the Number of Paths metric, and the Mean of Path Lengths metric are three attack graph-based security metrics that can extract security-relevant information. However, one's usage of these metrics can lead to misleading results. The Shortest Path metric and the Mean of Path Lengths metric fail to adequately account for the number of ways an attacker may violate a security policy. The Number of Paths metric fails to adequately account for the attack effort associated with the attack paths. To overcome these shortcomings, we propose a complimentary suite of attack graph-based security metrics and specify an algorithm for combining the usage of these metrics. We present simulated results that suggest that our approach reaches a conclusion about which of two attack graphs correspond to a network that is most secure in many instances.