Scalable Attack Path Finding for Increased Security

Goals

Software vulnerabilities can be leveraged by attackers to gain control of a host. Attackers can then use the controlled hosts as stepping stones for compromising other hosts until they create a path to the critical assets. Consequently, network administrators must examine the protected network as a whole rather than each vulnerable host independently. In recent years, logical attack graphs are used to find the most critical vulnerabilities and devise efficient hardening strategies for organizational networks. Most techniques for ranking vulnerabilities either do not scale well to medium-large networks with hundreds or thousands of hosts. (e.g. brute-force attack plan enumeration), or are not well suited for the analysis of logical attack graphs (e.g. centrality measures). Research is focused on improving the run time of cyberattack modeling tools.

Description

One solution explored by the researchers is reducing the graph representing the attacker steps. The reductions allow security admins to analyze bigger networks with complex attacker logic by simplifying the task of searching and eliminating optimal attacker paths. Results on an attack graph extracted from a network of a real organization with more than 300 hosts and 2400 vulnerabilities show that using the proposed graph reductions can improve the search time by a factor of 4 while maintaining the quality of the results.

In another solution, they suggest an analysis of the planning graph (from classical planning) derived from the logical attack graph to improve the accuracy of centrality-based vulnerability ranking metrics. The planning graph also allows efficient enumeration of the set of possible attack plans that use a given vulnerability on a specific machine. For this, they propose a set of centrality-based heuristics for reducing the number of attack plans and comparisons with previous vulnerability ranking metrics. Results show that metrics computed over the planning graph are superior to metrics computed over the logical attack graph or the network connectivity graph.

Researchers

Tom Gonda
tom.gonda@gmail.com

Prof. Bracha Shapira
bshapira@bgu.ac.il

Dr. Rami Puzis
puzis@bgu.ac.il

Publications

T. Gonda, R. Puzis, and B. Shapira, "Scalable Attack Path Finding for Increased Security," International Conference on Cyber Security Cryptography and Machine Learning (CSCML), 2017, 234-249.

T. Gonda, G.Shani, R. Puzis, B. Shapira, "Ranking Vulnerability Fixes Using Planning Graph Analysis," IWAISe-17, 2017.