Topic: Mathematical analysis of network telescope traffic for security metric discovery

Bradley Cowie and Barry Irwin

March 23, 2010

Abstract

Security Metrics are extremely topical within the Information Security field due to the need for organizations to better gauge their current operational security and to allow for tactical management decisions to be made with regards to Information Security within an organization. A potential avenue for generating security metrics is through the analysis of network traffic data captured by a Network Telescope. Network Telescopes grant insight into the nature of traffic trends on the Internet by recording traffic that is destined for unused parts of a networks address space. A specific example of this can be accrued in light of the dramatic increase in port 445 traffic post October 2008, this massive spike in port 445 traffic was caused by the Conficker worm attempting to infect machines through specifically crafted RPC's over port 445. It is clear that being able to identify these irregularities could aid CERTS in the early detection of anomalous activity. Thus, it would be useful if the detection of this anomalous behavior was an automated process. However, the generation of provable security metrics from Network Telescope data is a challenging task due to the difficulty involved in correctly identifying and quantifying potential vulnerabilities without causing excessive false-positives while ensuring that significant events are not neglected. In this paper, the authors intend to discuss a number of techniques of a mathematical and artificial intelligence nature to detect changes in network traffic that deviate from the expected norm, that consider the clipping level issue and the time taken to process large data sets through sensible heuristic generation. Potential weaknesses of these techniques will be identified together with the appropriate domains for said techniques. Initially the researchers intend to use a manual processes to determine sensible heuristics for example: sudden spikes in traffic on ports with traditionally low traffic frequencies or or a change in top port frequencies. Once a number of manual heuristics have been identified, the focus is to be shifted towards methods for efficient heuristics automation.