Introduction: When inspecting the traffic occurring in the Internet, we notice that a significant amount of it is caused by scanning, (D)DoS attacks, and other malicious causes. Because of the ubiquitous nature and its variable forms of appearance, this traffic is called Internet Background Radiation (IBR). To understand the causes of IBR, a detector software was developed for classifying the one-way flows occurring in the analysed traffic. To match the analysed one-way flows into defined classes, the IBR detector is based on a ruleset.

Approach/Technologies: A first goal is to evaluate if the rules match most of the one-way flows correctly. The second goal is to explain the causes of a peak in the analysed periods. In a first step, all flow belonging to a specific class is sorted out. The second step is the execution of the Frequent Item-set Mining (FIM) analysis applied to the flow and sign files. For statistical purposes, a sign statistic is created in a third step.

Result: The results of the FIM analysis have proven that the inspected flow-item sets are correctly classified. The second goal was not reached, because the FIM analysis did not reveal the causes of the peaks in all periods. A significant peak is detected in the item sets of the other malicious class. It is caused by clients trying to contact the server swisstime.ethz.ch on port 37, but the server only serves NTP and not the old Time Protocol. The sign statistics over a whole interval allows the calculation of the rule effectiveness of backscatter class, which shows that the rule containing the “backsc” sign is not very effective and matches less than 0.1% of flows to this class. On the other hand, the rule containing only the ICMP sign assigns the most flows to the backscatter class.

Evaluating Internet Background Radiation Detector Rules

This illustration shows a default netflow setup.

This illustration shows the data processing cycle of the project. Grey arrows mark the processing with a tool, the other colours mark the input files.

This chart shows all flow-item sets found in the interval of August 2008 of the other malicious class.