Distributed monitoring and analysis for reactive security

Tobias Limmer and Falko Dressler

University of Erlangen-Nuremberg, Department of Computer Science 7
(tobias.limmer| dressler){ at } informatik.uni-erlangen.de

An ever growing number of attacks to sites on the Internet increases the need for effective systems to detect those incidents and initiate countermeasures. Botnets are one of the most successful methods used by hackers. Those networks are difficult to detect and neutralize, but an especially difficult task is to find the individuals controlling the attacking hosts. A crucial part of successful dissection is the analysis of monitored data in several separate networks. Recently, we introduced our monitoring toolkit Vermont to enable distributed aggregation of such information.

Analysis of network monitoring data can be divided into two different types: payload-based and flow-based analysis. On the one hand, network monitors like Snort and Bro analyze complete network packets including payload. In this area usually signature-based detection methods are used. On the other hand, flow-based analysis summarizes monitored packet data to only include header information and to aggregate packets with common attributes to one record. This method achieves great information reduction but still provides enough data for following analysis to generate meaningful results [1]. It is mostly used in high-speed environments, where payload-based monitoring is not suitable due to performance problems. The most popular data format for transferring flow-based data is Cisco's Netflow v9, which is widely supported in hardware-based routers, and its successor IP Flow Information Export (IPFIX).

We are using Vermont, which runs under Unix-based operating systems, for flow-based analysis of network streams. It supports direct observation of packet data using the PCAP system library with subsequent aggregation and export as IPFIX flows. Special attention was paid to high flexibility and support of dynamic reconfiguration of its aggregation parameters. The application is also able to receive IPFIX flows, so it is hierarchically stackable. This enables it to be used in distributed high bandwidth environments, as load can be shared among several hosts. For example, the tasks for portscan detection, statistical analysis and anomaly detection can be performed on separate hosts, which work on identical data. If the task is still computationally too expensive, it could be split up in two parts and executed on two machines. Further possibilities of attack detection lie in the areas of detecting DoS-attacks, vertical and horizontal portscans, hosts sending spam mails or hosts, just in the process of being infected when downloading malware code. Those methods benefit from distributed monitoring stations which gather data in different networks and forward it to a centrally managed correlation system. Possible reactions to detected incidents may include the reconfiguration of firewalls which could help to prevent malware from spreading or to prevent the overload of analysis systems from a targeted DoS attack to cover more subtle attacks.

References

[1] Falko Dressler and Gerhard Münz: *Flexible Flow Aggregation for adaptive Network Monitoring*, pages 702-709 in *31st IEEE Conference on Local Computer Networks (LCN): 1st IEEE LCN Workshop on Network Measurements (WNM 2006)*, Tampa, Florida, November 2006.