Towards Effective Trust-Based Packet Filtering in Collaborative Network Environments

Overhead network packets are a big challenge for intrusion detection systems (IDSs), which may increase system burden, degrade system performance, and even cause the whole system collapse, when the number of incoming packets exceeds the maximum handling capability. To address this issue, packet filtration is considered as a promising solution, and our previous research efforts have proven that designing a trust-based packet filter was able to refine unwanted network packets and reduce the workload of a local IDS. With the development of Internet cooperation, collaborative intrusion detection environments (e.g., CIDNs) have been developed, which allow IDS nodes to collect information and learn experience from others. However, it would not be effective for the previously built trust-based packet filter to work in such a collaborative environment, since the process of trust computation can be easily compromised by insider attacks. In this paper, we adopt the existing CIDN framework and aim to apply a collaborative trust-based approach to reduce unwanted packets. More specifically, we develop a collaborative trust-based packet filter, which can be deployed in collaborative networks and be robust against typical insider attacks (e.g., betrayal attacks). Experimental results in various simulated and practical environments demonstrate that our filter can perform effectively in reducing unwanted traffic and can defend against insider attacks through identifying malicious nodes in a quick manner, as compared to similar approaches.