A Study of Attack Prediction Using Network Alerts

Toshitaka Mori (1210055)

School of Information Science,
Japan Advanced Institute of Science and Technology

February 12, 2014

Keywords: Malware, IDS, Attack Prediction.

Cyber attacks have increased in recent years. In particular, the attack using an automated program like malware is increased, and it causes serious damage. Intrusion Detection System (IDS) is one of the effective countermeasures for detecting malware. However, since IDS generates enormous alerts, network administrator always bothers with how to cope with the alerts. To address this problem, Cipriano et al. proposed a method called "Nexat" to predict the attack based on IDS alerts. However, it is not clear whether Nexat is effective for the prediction of malware that is not always true that is occer IDS alerts.

In this paper, we evaluate Nexat by using the CCC DATAset 2011 which is one of the malware research data sets, in order to consider how effective the prediction of malware is. Usually, IDS does not output malware download as an alert. Therefore, we create local IDS rules for detecting the malware download, and it is used as training data. On the other hand, we do not use the local IDS rules for prediction. As a result, we succeed in predicting malware with a probability of about 70%.

In addition, we propose an improved and simplified algorithm based on Nexat. Considering that malware is a robot program, we improve the prediction phase mainly. As a result, we are succeed in malware prediction with a probability of about 90%. Moreover, we evaluate false negative rate, and confirm that it is a low value as Nexat.